Supreme Court, U.S.
FILED
06-436 SEP 25 2008
OFFICE OF THE CLERK

No. ——

In the Supreme Court of the United States

LYMAN WAGERS,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit

PETITION FOR WRIT OF CERTIORARI

H. LOUIS SIRKIN
Counsel of Record
JENNIFER M. KINSLEY
SCOTT RYAN NAZZARINE
SIRKIN, PINALES & SCHWARTZ LLP
105 WEST FOURTH STREET, SUITE 920
CINCINNATI, OH 45202-2726
(513) 721-4876
(513) 721-0876 FAX

Counsel for Petitioner

Becker Gallagher Legal Publishing, Inc. 800.890.5001

QUESTIONS PRESENTED

1. Whether an affidavit for a search warrant in which the basic allegation in support of probable cause is a person's prior subscription to a "mixed" website, containing both lawful and unlawful content, without any allegation that the person downloaded, possessed, or even viewed child pornography from the website while a member, is sufficient to establish probable cause to search and seize that person's computer and related records from his home and elsewhere?

TABLE OF CONTENTS

Page

QUESTIONS PRESENTED i

TABLE OF CONTENTS ii

TABLE OF AUTHORITIES iv

OPINIONS BELOW 1

JURISDICTION 1

CONSTITUTIONAL AND STATUTORY PROVISIONS 2

STATEMENT OF THE CASE 2

REASONS FOR GRANTING THE WRIT 5

I. Reasonable Jurists Are in Disagreement About Whether a Person's Prior Membership in a "Mixed" Website that Contained Both Lawful and Unlawful Content is Sufficient to Establish Probable Cause to Search that Person's Computer 5

II. The Issues Presented in this Petition Present an Important, Exceptional, and Recurring Issue of Federal Law Due to the Increased Proliferation and Importance of Computers in Our Society, the Increased Emphasis and Governmental Priority on Prosecution for Internet Child Pornography Cases, and the Fact That Probable Cause and Suppression

Issues Remain Unsettled in the Context of Membership with Online Pornography Groups. . 27

CONCLUSION 30

TABLE OF AUTHORITIES

Cases

Florida v. Riley, 488 U.S. 445 (1989) 7

Illinois v. Gates, 462 U.S. 213 (1983) 5

Mapp v. Ohio, 367 U.S. 643 (1961) 6

Maryland v. Pringle, 540 U.S. 366 (2003) 6

Red Lion Broadcasting Co. v. FCC,
395 U.S. 367 (1969) 29, 30

Reno v. ACLU, 521 U.S. 844 (1997) 28

United States v. Bailey,
272 F.Supp.2d 822 (D.Neb. 2003) 25

United States v. Coreas,
419 F.3d 151 (2nd Cir. 2005),
reh'g denied, 426 F.3d 615 (2nd Cir. 2005),
reh'g en banc denied, 430 F.3d 73 (2nd Cir. 2005),
cert. denied, 126 S.Ct. 2861 (2006) . . . . . *passim*

United States v. Coreas,
426 F.3d 615 (2nd Cir. 2005),
reh'g en banc denied, 430 F.3d 73 (2nd Cir. 2005),
cert. denied, 126 S.Ct. 2861 (2006) . . . . . *passim*

United States v. Froman, 355 F.3d 882 (5th Cir. 2004) . 25

United States v. Gourde,
382 F.3d 1003 (9th Cir. 2004),
rev'd en banc, 440 F.3d 1065 (9th Cir. 2006) . . *passim*

United States v. Gourde, 416 F.3d 961 (9th Cir. 2005) . 15

United States v. Gourde,
440 F.3d 1065 (9th Cir. 2006) (*en banc*), *petition for cert. filed July 7, 2006* . . . . . *passim*

United States v. Kunen,
323 F.Supp.2d 390 (E.D.N.Y.) 25

United States v. Martin,
426 F.3d 68 (2nd Cir. 2005),
reh'g denied, 426 F.3d 83 (2nd Cir. 2005),
reh'g en banc denied, 430 F.3d 73 (2nd Cir. 2005),
cert. denied, 126 S.Ct. 2861 (2006) . . . . . *passim*

United States v. Martin,
426 F.3d 83 (2nd Cir. 2005),
reh'g en banc denied, 430 F.3d 73 (2nd Cir. 2005),
cert. denied, 126 S.Ct. 2861 (2006) . . . . . *passim*

United States v. Martin,
430 F.3d 73 (2nd Cir. 2005),
cert. denied, 126 S.Ct. 2861 (2006) 18, 24

United States v. Perez,
247 F.Supp.2d 459 (S.D.N.Y. 2003) 18, 24, 25

United States v. Strausser,
247 F.Supp.2d 1135 (E.D.Mo. 2003) 24

United States v. United States District Court for E.D. Michigan,
407 U.S. 297 (1972) 7

United States v. Wagers,
339 F.Supp.2d 934 (E.D.Ky 2004) . . . . . *passim*

United States v. Wagers,
452 F.3d 534 (6th Cir. 2006) . . . . . *passim*

United States v. Weber,
923 F.2d 1338 (9th Cir. 1990) 10

Ybarra v. Illinois, 444 U.S. 85 (1979) 6

Statutes

18 U.S.C. § 2251, *et seq.* 29

18 U.S.C. § 2252 . . . . . 2, 15

18 U.S.C. § 2257 29

18 U.S.C. § 2257A 29

18 U.S.C. § 3211 1

28 U.S.C. § 1254(1) 1

47 U.S.C. § 223 29

47 U.S.C. § 231 29

Pub. L. No. 108-21, 117 Stat. 650 29

Other

U.S. CONST. amend. IV. 2, 5, 6

Fed. R. Crim. P. 41. 6

Barry M. Leiner *et al.*, *A Brief History of the Internet* (Ed. 3.32) at http://www.isoc.org/internet/history/brief.shtml# References (Dec. 10, 2003) 28

Child Porn Rising on the Web, at http://www.csmonitor.com/2005/0818/p01s01-stct.html 29

Internet Pornography Statistics: 2003, at http://www.healthymind.com/s-porn-stats.html 28

March 2006 Web Server Survey, at http://news.netcraft.com/archives/2006/03/06/march_2006_web_server_survey.html 27, 28

PETITION FOR WRIT OF CERTIORARI

Now comes the Petitioner, Lyman Wagers, and respectfully requests that a writ of certiorari be issued to review the Opinion of the United States Court of Appeals for the Sixth Circuit, decided on June 27, 2006, and reported at *United States v. Wagers*, 452 F.3d 534 (6th Cir. 2006).

OPINIONS BELOW

The Opinion of the United States Court of Appeals for the Sixth Circuit affirming the district court's denial of Mr. Wagers's motion to suppress is reported at *United States v. Wagers*, 452 F.3d 534 (6th Cir. 2006) (hereinafter, "*Wagers II*"). This Opinion is reprinted in its entirety at Appendix A, pp. 1a-15a. The District Court's Memorandum Opinion and Order denying Mr. Wager's motion to suppress is reported at *United States v. Wagers*, 339 F.Supp.2d 934 (E.D.Ky 2004) (hereinafter, "*Wagers I*"). The district court's Opinion and Order is reprinted in its entirety at Appendix C, pp. 24a-41a. The district court's judgment is reprinted in its entirety at Appendix B, pp. 16a-23a.

JURISDICTION

The decision of the court of appeals was issued on June 27, 2006. The Supreme Court has jurisdiction under 28 U.S.C. § 1254(1) to review this Petition.

The district court had jurisdiction to hear the case under 18 U.S.C. § 3231.

CONSTITUTIONAL AND STATUTORY PROVISIONS

This case involves the Fourth Amendment to the United States Constitution, which provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

This case also involves the federal statute, 18 U.S.C. § 2252, entitled Certain activities relating to material involving the sexual exploitation of minors, which is reprinted in its entirety at App. G, pp. 131a-135a.

STATEMENT OF THE CASE

Petitioner Lyman Wagers was arrested for possession of child pornography in April 2004, a charge to which he ultimately pleaded guilty and for which he was sentenced to 180 months in prison. *Wagers II*, 452 F.3d at 536. (Apx. A, p. 2a). The charges arose from the execution of two separate search warrants, one at Wagers's residence and one at his business office, as well as a separate search warrant that was served on America Online, the provider of Wagers's e-mail account. *Id.* at 536-37. (Apx. A, p. 3a). Three separate affidavits underlie the search of Wagers's home and office: 1) the affidavit supporting the warrant for Wagers's residence ("the Mimosa Lane affidavit") (reprinted in its entirety at App. D, pp. 42a-79a); 2) the affidavit supporting the warrant for Wagers's place of business ("the Harrodsburg Road affidavit") (reprinted in its entirety at App. E, pp. 80a-118a); and 3) the affidavit supporting a warrant to search records at

America Online's corporate offices ("the e-mail account affidavit") (reprinted in its entirety at App. F, pp. 119a-130a).

The first search was executed at Wagers's home on April 5, 2004, by federal agents. *Wagers II*, 452 F.3d at 537 (Apx. A, p. 3a). The search warrant was based upon information that Wagers had purchased short-term subscriptions to three websites, http://www.redlagoon.com, http://www.video2000.com, and http://www.darkfeeling.com, which were later found to contain both sexually explicit lawful content and child pornography. (Mimosa Lane Affidavit ¶¶ 24-41, Apx. D, pp. 56a-65a). Significantly, however, the agents had no information that Wagers had ever viewed the websites or that his memberships were even active at a time when the unlawful images were displayed online. (Mimosa Lane Affidavit ¶ 14, Apx. D, p. 51a); *see also Wagers II*, 452 F.3d at 537 (Apx. A, p. 4a).

Two days later, agents obtained a second search warrant for Wagers's business office. (Harrodsburg Road Affidavit, Apx. E). Again, the authorities had no information linking Wagers's memberships to actual online child pornography. Instead, the affidavit in support of the search warrant for Wagers's business contained virtually identical information to that contained in the request to search Wagers's residence, supplemented with the additional allegation that a cursory examination of Wagers's home computer revealed sexually explicit images of children. (Harrodsburg Road Affidavit ¶ 2, Apx. E, pp. 83a-84a and generally).

A third search warrant was issued and executed on April 8, 2004. This time, agents searched e-mail records maintained by America Online, the alleged provider of Wagers's e-mail account. (E-mail Account Affidavit, Apx.

F). They did so without any specific articulated reason to believe that Wagers used his e-mail account to commit the alleged offenses outside of the generalized experience of the investigating agent that unlawful images are occasionally exchanged by e-mail. *Id.*

The affidavits in support of these search warrants alleged that Wagers purchased subscriptions to three computer websites that were later found to display sexually explicit images of children; they did not, however, suggest that Wagers had viewed the websites or had ever accessed any unlawful content. *Wagers II*, 452 F.3d at 537 (Apx. A, p. 4a). In fact, the affidavits in support of the search warrants conceded a lack of proof that child pornography appeared on the websites at the time Wagers was a member. *Id.*

Nevertheless, Wagers was indicted by a federal grand jury on May 6, 2004 with one count of conspiracy to receive child pornography, eleven counts of receiving child pornography, and one count of possessing child pornography. *Id.* The indictment was later superseded to add seven additional receiving charges, and again amended a second time to correct a defect in the explanation of penalties section.

Following the second superseding indictment, Wagers moved to suppress evidence seized from his home and office during the execution of the search warrants. *Id.* The district court denied the motion to suppress. *See id.* In a published opinion, the district court explained that "there is no need to make 'inferences upon inferences' in this case.... [T]he only inference to be made herein is that the Defendant accessed child pornography on the websites at issue at some point." *Wagers I*, 339 F.Supp.2d at 941 (Apx. C, p. 36a). The court reasoned that Wagers had previously been convicted of child pornography, that he had Internet connections at the places to

be searched, that "he purchased several subscriptions at varying times to the websites at issue; and those websites, at various points in time, contained various child pornographic material." *Id.* Thus, the court concluded, the magistrate has a substantial basis for finding probable cause. *Id.* Following the district court's opinion and order, Wagers entered a plea of guilty to all 21 counts, conditioned on his ability to appeal the judge's decision denying the motion to suppress. *Wagers II*, 452 F.3d at 537 (Apx. A, p. 4a). Wagers was sentenced on February 11, 2005 to 180 months in prison. *Id.*

Wagers timely appealed his conviction to the United States Court of Appeals for the Sixth Circuit, arguing that the district court erred in denying his motion to suppress because the three search warrants were not supported by probable cause. *Id.* The Sixth Circuit issued an opinion on June 27, 2006, affirming the district court's denial of the motion to suppress. *Id.* at 536 (Apx. A, pp. 1a-2a). Mr. Wagers now respectfully petitions this Court for a writ of certiorari to review that opinion.

REASONS FOR GRANTING THE WRIT

I. Reasonable Jurists Are in Disagreement About Whether a Person's Prior Membership in a "Mixed" Website that Contained Both Lawful and Unlawful Content is Sufficient to Establish Probable Cause to Search that Person's Computer.

The Fourth Amendment to the United States Constitution protects individuals from unreasonable searches and seizures. U.S. CONST. amend. IV. Subject to few exceptions, a warrant is generally required to insure that a particular search comports with the Fourth Amendment reasonableness requirement. *Id.*; *Illinois v. Gates*, 462 U.S. 213 (1983).

Furthermore, that warrant must comply with certain procedural and constitutional safeguards, including the requirements that it be supported by probable cause and that it describe both the place to be searched and the items to be seized with particularity. U.S. CONST. amend. IV. Absent these safeguards, a warrant is invalid, and the results of any search must be suppressed. *Mapp v. Ohio*, 367 U.S. 643 (1961).

The standard required to issue a search warrant is probable cause. *See* Fed. R. Crim. P. 41. "[P]robable cause is a fluid concept–turning on the assessment of probabilities in particular factual contexts–not readily, or even usefully, reduced to a neat set of legal rules." *Gates*, 462 U.S. at 232. Presented with a warrant application, a judge must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him ... there is a fair probability that contraband or evidence of a crime will be found in a particular case." *Id.* at 238. "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others." *Id.* at 239.

Although probable cause is incapable of a precise definition or quantification, the Supreme Court has repeatedly noted that "[t]he substance of all definitions of probable cause is a reasonable ground for belief of guilt and that the belief of guilt must be particularized with respect to the person to be searched or seized." *Maryland v. Pringle*, 540 U.S. 366, 371 (2003) (internal quotations and citations omitted). Thus, "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). Ultimately, "[t]he long-prevailing

standard of probable cause protects citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime, while giving fair leeway for enforcing the law in the community's protection." *Pringle*, 540 U.S. at 370 (internal quotations and citations omitted).

However, it must be noted that particular care must be taken when the warrant authorizes search of a home or residence. This is true because expectations of privacy, which are core to Fourth Amendment protection, are heightened in the home. *Florida v. Riley*, 488 U.S. 445, 453 (1989) (O'Connor, J., concurring). In fact, "physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed." *United States v. United States District Court for E.D. Michigan*, 407 U.S. 297, 313 (1972).

In the instant case, three separate affidavits ostensibly established the requisite probable cause to search Wagers' home and office: "the Mimosa Lane affidavit," "the Harrodsburg Road affidavit," and "the e-mail account affidavit." Collectively, these affidavits establish that during March, July, and August 2003, undercover agents visited three separate websites–Red Lagoon, Video 2000, and Dark Feeling–which were suspected of containing child pornography. (Mimosa Lane Affidavit ¶ 26, Apx. D, p. 58a-61a; Harrodsburg Road Affidavit ¶ 26, Apx. E, p. 97a-100a); *see also Wagers II*, 452 F.3d at 536-37 (Apx. A, p. 6a). While viewing the websites, the agents discovered that some, but not all, of the images displayed on the sites constituted child pornography. *Id.*

Records from the websites' billing service reflected that Wagers held short-term subscriptions to each of these websites. According to the affidavits, Wagers purchased a

one-to-two month membership to the website Red Lagoon on June 30, 2002. *See Wagers II*, 452 F.3d at 537, 538 (Apx. A, p. 2a-6a). The undercover agent who viewed the Red Lagoon website did so on March 26, 2003, approximately eight months after Wagers' subscriptions had expired. *Id.* In addition, Wagers purchased two one-to-two month memberships to the website Video 2000. The first subscription began March 22, 2003 and the second subscription began on June 3, 2003. *Id.* The undercover agents, however, only viewed the Video 2000 website on or after August 1, 2003, when Wagers' subscriptions had expired. *Id.* Wagers also purchased a one-to-two month subscription to the Dark Feeling website on April 15, 2003. *Id.* The undercover agent visited the Dark Feeling website on or after July 21, 2003, several months after the expiration of Wagers' membership. *Id.*

Based on the allegations contained in the several affidavits that Mr Wagers had paid to subscribe to several websites which were confirmed to later contain images of child pornography, the fact that Mr. Wagers also had a previous conviction for possession of child pornography in 1997, and the agents' experience that collectors of child pornography often maintain evidence of their crimes on their computers, the magistrate judge issued warrants to search Wagers's home and business computers. *Id.*

However, Mr. Wagers maintained on appeal that, given the undisputed facts and timeline, the affidavit failed to set forth any facts connecting Wagers' subscriptions to websites that contained child pornography at the time Wagers was a member, nor did they establish a fair probability that he was likely to possess such images at the time the warrants were executed. *See id.* at 538-43 (Apx. A, p. 5a). In fact, the affidavits failed to prove that Wagers ever even accessed the

webpages while his subscriptions were activated. *See id.* at 537 (Apx. A, pp. 5a, 4a) ("The warrants and their supporting affidavits alleged that Wagers had bought subscriptions to websites that were found at a later date to display child pornography. They did not specifically allege that Wagers had viewed the sites or that he had accessed unlawful content on them."). Even the affiant himself frankly admitted as much when he stated: "the federal agents have no way of ascertaining the actual contents of each website on the various dates customer would have visited the website." (Mimosa Lane Affidavit ¶ 14, Apx. D, p. 51a).

Furthermore, even if it is conceded, *arguendo*, that there was probable cause to believe these websites did contain child pornography at a time when Wagers had subscriptions to them and that he in fact accessed these sites, the websites were at most "mixed sites" that contained both legal and illegal images and content. Clearly, this fact further diminishes any reasonable probability to believe that Wagers actually accessed and possessed any contraband materials, much less establishes probable cause to believe that he downloaded and then maintained child pornography on his computers for a minimum of eight months prior to the search.

In other words, in order to ostensibly establish probable cause in this case, several inferences must be stacked upon one another. First, it must be inferred that during the time period that Wagers subscribed to the websites, they contained child pornography. Second, it must be inferred that Wagers actually visited the websites once he obtained the subscriptions. Third, it must be inferred that, when he did visit the websites, he chose to view the illegal contents of those websites rather than the legal contents. Fourth, it must be inferred that Wagers downloaded illegal materials from the websites. Finally, it must be inferred that Wagers kept the

images at either his home or his office from the time that he would have been able to download them until the time the search warrants were executed. The federal courts have commented on, and routinely rejected, search warrant affidavits which require a similar "stacking" of inferences to establish probable cause. *See, e.g., United States v. Weber*, 923 F.2d 1338, 1345 (9th Cir. 1990) ("with each succeeding inference, the last reached is less and less likely to be true. Virtual certainty become probability, which merges into possibility which fades into chance.").

Nonetheless, the Sixth Circuit Court of Appeals determined that the district court did not abuse its discretion in denying Wagers's motion to suppress evidence gathered pursuant to the search of his home and office. *Wagers II*, 452 F.3d at 543 (Apx. A, p. 15a). Specifically, in response to Wagers's argument that the agents' subscriptions post-dated his own and thus failed to establish probable cause that any child pornography was present on the sites at the time Wagers had access to them, the court noted:

> Whether or not there was an actual overlap between subscriptions, an inference based on the difference of a few days–in the case of video2000.com–or of roughly 30 days–in the case of darkfeeling.com–is not very hard to make, even setting aside the perhaps more tenuous inference based on research on redlagoon.com that was five months after Wagers's known use.

Id. at 538 (Apx. A, p. 6a).

Similarly, in response to Wagers's related argument (opposed factually by the government) that probable cause was further lacking because the website was a "mixed site"

(i.e., contained both legal and illegal images), the Sixth Circuit noted that neither party offered clear support in the record for their position, but that this issue was not dispositive because "[p]robable cause to search for illicit pornography in Wagers's home, office, and email account existed even without a statement that these three websites contained only illegal images." *Id.* at 538-39 (Apx. A, pp. 6a-7a). Furthermore, the court noted that this conclusion was "especially strong in light of the temporal analysis" due to the "proximity in time" between the agents' and Wagers's subscriptions to the site. *Id.* Thus, upon a *de novo* review of the reasonableness of the search, the Sixth Circuit ultimately concluded that, under the totality of the circumstances, the district court properly denied Wagers's motion to suppress evidence. *Id.* at 536-38 (Apx. A, pp. 1a-5a).

While the application of clearly established Fourth Amendment law to the relevant facts of a particular case is perhaps, in and of itself, insufficient to warrant certiorari review, the diversity of opinions by federal judges on this particular issue, combined with the proliferation of child pornography on the Internet, the increased emphasis on prosecution for such crimes, and the unsettled nature of Fourth Amendment law as it regards a person's involvement or association with an activity having both legal and illegal aspects, demands clarification by this Court and the granting of a writ of certiorari in this case. Indeed, as shown below, reasonable jurists have concluded on numerous occasions that similar, if not indistinguishable, circumstances as those in the instant case, fail to establish probable cause to believe that a crime has been committed, whereas other courts have found probable cause on even more tenuous evidential inferences. This split–or, perhaps more accurately, lack–of authority has created conflicting opinions and disorder in the lower courts on this constitutional issue of profound national importance.

The case of *United States v. Micah Gourde* is perhaps the most clear cut–though by no means the only–illustration of the *lack* of clarity, consistency, or reasonable consensus regarding the determination of probable cause arising from an individual's subscription to a mixed content website. *See generally United States v. Gourde*, 382 F.3d 1003 (9th Cir. 2004), *rev'd en banc*, 440 F.3d 1065 (9th Cir. 2006) (hereinafter, "*Gourde Panel*"); *United States v. Gourde*, 440 F.3d 1065, 1067 (9th Cir. 2006) (*en banc*), *petition for cert. filed July 7, 2006* (hereinafter, "*Gourde en banc*"). Arising under circumstances very similar to those presented in the instant petition, the *Gourde* case, as shown below, resulted in at least five different opinions throughout its procedural history on the issue of whether a person's past subscription to a website later found to contain a mixture of adult pornography, child pornography, and child erotica was sufficient to establish probable cause to search that person's residence and computers.

The *Gourde* case initially began its arduous journey through the courts in May 2002, when the FBI applied for a warrant to search Gourde's residence and seize his computer for evidence that he had "probably caused the uploading, downloading, and transmission of child pornography over the Internet." *See Gourde en banc,* 440 F.3d at 1067. The investigation that ultimately led to the search warrant had begun in August 2001 when an undercover FBI agent discovered and joined a website called "Lolitagurls.com." *Id.* Following an investigation, the FBI identified the owner of the website and, pursuant to a warrant, conducted a search of his home. *Id.* Then, in response to a follow-up grand jury subpoena to the credit card processing company used by Lolitagurls.com, the government learned that Gourde had been a subscriber to Lolitagurls.com from November 2001

until January 2002, when the FBI shut down the site. *Id.* at 1067-68.

Based on the above information, combined with "extensive background information on computers and the characteristics of child pornography collectors" in the FBI agent's affidavit, a magistrate judge issued a warrant to search Gourde's residence and seize his computer, which was later found to contain over 100 images of child pornography. *Id.* Subsequently, Gourde filed a motion to suppress the images found on his computer, and the district court conducted a suppression hearing. *Id.* at 1068-69. At the hearing, one of the FBI agents involved in the investigation admitted that the agency had the means to track Gourde's actual usage of the website during its four-month investigation of Lolitagurls.com, but conceded that the affidavit in support nonetheless contained "no evidence that Gourde had 'actually downloaded, received, transmitted or in any way otherwise possessed child pornography,'" nor did the affidavit indicate that the child pornography images appeared on the site when Gourde had access to it. *Gourde Panel*, 382 F.3d at 1007.

The district court judge, restricting his ruling to "the face of the affidavit," ultimately determined that the affidavit supported a fair probability that evidence of a crime would be found on Gourde's computer. *Gourde en banc,* 440 F.3d at 1069. The judge "applied a 'common sense approach' to conclude that evidence of a subscription to even a 'mixed' site–one that offered both legal adult pornography and illegal child pornography–provided the necessary 'fair probability' to 'look further,'" and thus denied the motion to suppress. *See Gourde Panel*, 382 F.3d at 1008. After this ruling, Gourde pleaded guilty to one count of possession of child pornography, but his guilty plea was conditioned on his right

to appeal the district court's denial of his motion to suppress. *Id.*

On appeal, the Ninth Circuit Panel reversed the judgment of the district court, ruling unanimously that the affidavit in question failed to present sufficient indicia of probable cause to believe that evidence of a crime would be found on Gourde's computer. *Id.* at 1009-14. The panel reasoned that "the chain of inferences that the government asks us to draw is unprecedentedly lengthy and improbable" and that "[a]n affidavit establishing that it is possible, with some straining, to *infer* that Gourde–along with every other member of every site on the Internet containing what appears to be child pornography–might possess child pornography is not enough to justify a warrant to search Gourde's home and seize his computer." *Id.* at 1011 (emphasis in original). Ultimately, the panel concluded that "the affidavit here revealed only that Gourde had subscribed, and thereby received access, to a mixed-pornography website, which is insufficient to create a fair probability that evidence of possession of child pornography would be found on Gourde's computer." *Id.* at 1013.

One Judge wrote a concurring opinion in which he agreed with the panel opinion's persuasive application of precedent, but noted that "were [he] free to look only at first principles and Supreme Court precedent, [he] would be more inclined to decide that there was probable cause for this search." *Id.* at 1014-16 (Gould, J., concurring). Judge Gould stated that, were one to examine this case "using only the Supreme Court's 'fair probability' standard in the general probable cause context, in [his] view it would be permissible to conclude that law enforcement officials had adequate cause to gain the warrant to search Gourde's computer." *Id.* at 1015. Nonetheless, under relevant precedent, Judge Gould

concurred in the judgment that the district court erred in refusing to suppress because the affidavit failed to present sufficient indicia of probable cause. *Id* at 1014.

Following the panel's ruling, the Ninth Circuit voted to rehear the *Gourde* case *en banc*, *United States v. Gourde*, 416 F.3d 961 (9th Cir. 2005). The Ninth Circuit *en banc* ultimately overturned the panel's decision by concluding that the affidavit at issue contained sufficient facts to support the magistrate judge's issuance of the search warrant and the district court's finding of probable cause. *See generally Gourde en banc*, 440 F.3d 1065. The *en banc* court reasoned that the affidavit was sufficient to establish probable cause because it "move[d] from one certainty, that child pornography was on the website, to another–that Gourde had access and wanted access to these illegal images," and that Gourde had the means to receive and possess images in violation of 18 U.S.C. § 2252. *Id.* at 1070. The court explained that "Gourde's status as a member [of the website's subscription service] manifested his intention and desire to obtain illegal images." *Id.*

The court further explained that given the "triad of solid facts" revealed by the affidavit–that the site had illegal images on it, that Gourde intended to have and wanted to have access to these images, and that the images would be almost certainly retrievable from his computer if he had received them–then "the only inference the magistrate judge needed to make to find probable cause was that there was a 'fair probability' Gourde had, in fact, received or downloaded images." *Id.* at 1071. The court determined that this was a reasonable inference because it "neither strains logic nor defies common sense to conclude, based on the totality of the circumstances, that someone who paid for access for two months to a website that actually purveyed child pornography probably had viewed

or downloaded such images onto his computer." *Id.* The *en banc* court thus held that, giving deference to the magistrate and applying a practical, common sense conception of probable cause, under the totality of the circumstances the search warrant was supported by probable cause. *Id.*

While the *en banc* majority opinion in Gourde "conclude[d] that the affidavit made out probable cause by assuming that anyone who subscribes to an [I]nternet site with both legal and illegal material must collect illegal material from the site," Judge Kleinfeld's dissent vigorously argued that "[t]his assumption stacks inference upon inference until the conclusion is too weak to support the invasion of privacy entailed by a search warrant." *Gourde en banc,* 440 F.3d at 1084 (Kleinfeld, J., dissenting). Judge Kleinfeld explained that, under a common sense approach, there was no probable cause to search Gourde's computer for evidence of a crime because "Gourde might have been using the website to look at the legal rather than the illegal material" and even if he had subscribed in order to look at illegal child pornography, the affidavit failed to demonstrate that Gourde actually received or possessed any such images. *Id.* at 1078. Furthermore, Judge Kleinfeld argued, "there were indications that supported the inference that some or most subscribers would want the site for access to legal pornography." *Id.* at 1079. Ultimately, Judge Kleinfeld determined that "the majority err[ed] in concluding that there was probable cause for a search because its inferences depend on unarticulated assumptions that do not make sense." *Id.* at 1077.

In a separate dissent, Judge Reinhardt argued that "when the government's failure to examine the critical evidence [whether Gourde had in fact downloaded illegal images to his computer] is considered along with the limited information proffered in the affidavit, it cannot be said that, all things

considered, there was a 'fair probability' that evidence ... would be found on [Gourde's] computer." *Gourde en banc*, 440 F.3d 1076 (Reinhardt, J., dissenting). Judge Reinhardt stated that, had the government *not* possessed potentially dispositive evidence whether Gourde actually downloaded child pornography, "the evidence that is set forth in the affidavit *might* have been sufficient to support a finding of probable cause." *Id.* at 1075 (emphasis in original). He explained that "membership in a mixed website alone" would "perhaps" be sufficient to establish probable cause; "perhaps not." *Id.* at 1077.[1] Ultimately, Judge Reinhardt explained, "I have some doubts about the question but I need not decide it here." *Id.* at 1075 n.1.

While Judge Reinhardt felt that he did not need to decide the question of whether membership in a mixed website alone was sufficient to establish probable cause to search that person's computer, many courts have been, and will be, faced with just this issue. And, as the varied, disjointed, and oftentimes conflicting opinions of the lower courts attempting to answer this and similar questions reveal, the issue is far from resolved. In fact, even when an Internet site may exclusively contain only illegal child pornography, reasonable jurists are nonetheless in disagreement about whether–absent any particularized evidence in the affidavit that the individual in fact accessed or possessed child pornography–membership or affirmative association with such a website in and of itself is sufficient to establish probable cause.

---

[1] Judge Reinhardt's footnote that "[a]lthough the majority labels the website a 'child pornography site,' it was in fact 'mixed'-that is, it contained both legal images (such as adult pornography) as well as illegal ones" bears emphasis at this point. *See id.* at 1077 n.3.

Several related cases from the Second Circuit explicitly and tellingly reveal the disorder, the lack of clarity, and the lack of consensus on this exact issue, thus further revealing the need for authoritative direction by the Supreme Court. *See generally, United States v. Martin*, 426 F.3d 68 (2nd Cir. 2005) ("*Martin I*"), *reh'g denied*, 426 F.3d 83 (2nd Cir. 2005) ("*Martin II*"), *reh'g en banc denied*, 430 F.3d 73 (2nd Cir. 2005) ("*Martin III*"), *cert. denied*, 126 S.Ct. 2861 (2006); *United States v. Coreas*, 419 F.3d 151 (2nd Cir. 2005) ("*Coreas I*"), *reh'g denied*, 426 F.3d 615 (2nd Cir. 2005) ("*Coreas II*") *reh'g en banc denied*, 430 F.3d 73 (2nd Cir. 2005), *cert. denied*, 126 S.Ct. 2861 (2006); *see also United States v. Perez*, 247 F.Supp.2d 459 (S.D.N.Y. 2003). Each of these cases (as well as several others) arose out of "Operation Candyman," an extensive government investigation of Internet child pornography which focused on a website and e-group known as "Candyman," and several related child pornography websites.[2] *See, e.g., Martin I*, 426 F.3d at 69-72, *Coreas I*, 419 F.3d at 151-54. The search warrants in all of these cases were authorized based on a single FBI agent's investigative findings and affidavit, but each was supplemented by additional facts specific to the particular defendant. *See id.* The FBI agent's affidavit indicated that each of the relative defendants likely possessed child pornography on their computer because various child pornography images had been sent through the e-group and each member of the Candyman group *automatically* received messages and image files when any other member posted an image or file. *See Martin I*, 426 F.3d at 70. However, it was later discovered at a *Franks* hearing in another related case

---

[2] "An e-group is an internet forum through which persons with similar interests can interact by e-mail and online 'chat,' and by posting messages, pictures, and videos to the group's website." *Martin I*, 426 F.3d at 70 n.1.

that the e-mail receipt by members was optional rather than automatic, and thus there was no proof that any individual member of the e-group actually received child pornography. *See Martin I*, 426 F.3d at 70-71; *Coreas I*, 419 F.3d at 153; *Coreas II*, 426 F.3d at 616 (noting that "once the false information provided by the FBI agent is excised, there remains no evidence whatever that the defendant in either case [Martin or Coreas] had actually downloaded any illegal visual depictions.").[3] Based on this newly discovered information, the various defendants moved to have the erroneous information removed from the affidavits and to suppress all evidence seized pursuant to the now-excised warrant applications. *See, e.g.*, *Martin I*, 426 F.3d at 72; *Coreas I*, 419 F.3d at 154-55.

Thus, the various courts were forced to confront the issue of whether there was sufficient evidence to establish probable cause based solely on membership in an Internet group that contained child pornography, without any evidence that any particular defendant actually possessed child pornography. As one court noted, "[o]nce the false statements of the FBI agent are excised," the only evidence that remains in these cases to establish probable cause that evidence of a crime exists "is the fact that Coreas and Martin had logged onto the respective websites and clicked the buttons indicating they wished to join. In neither case is there any evidence whatever

---

[3] Of course, the truthfulness or the recklessness of the affiant's presentation of facts in the Candyman cases is not particularly relevant to the issue presented in this Petition; however, the fact that the affidavits were excised in those cases is helpful here in that it narrows the issue to one that specifically focuses on whether membership in a website alone, without any allegations that the defendant actually downloaded or possessed child pornography, is sufficient to constitute probable cause under the Fourth Amendment.

that *anyone* on their premises ever downloaded any child pornography." *Coreas II*, 426 F.3d at 617. Despite the fact that the issue was so narrow and sharply focused, the Second Circuit was in utter disorder in trying to resolve this perplexing question.

In *Martin I*, a divided court concluded that the affidavit, after being corrected for error, still supported a finding of probable cause because it contained facts sufficient to conclude that "the overriding, if not the sole, purpose of the girls 12-16 e-group was illicit (to facilitate the receipt and distribution of child pornography)" and thus under the totality of the circumstances and applying common sense, there was a fair probability that "evidence of a crime would be found at Martin's home because *membership in the e-group reasonably implied use of the website*." 426 F.3d at 74-75 (emphasis added). The court explained that its holding "recognizes that, depending on the totality of the evidence proffered in the affidavit, a substantial likelihood of criminal activity may exist if an individual is a member of an [I]nternet e-group whose purpose is unlawful," and that "[a] contrary conclusion would unnecessarily hamper government investigations by fostering too restrictive a view of probable cause, and would conflict with the pragmatic, common-sense approach probable cause analysis that the Supreme Court requires." *Id.* at 76.

In a strongly worded dissent, Judge Pooler opined that "today the majority announces a dangerous precedent," in part because the reasoning "relies on numerous unreasonable inferences to gloss over the deficiencies in the corrected affidavit," and counter to the Fourth Amendment's protection against unreasonable searches and seizures. *Id.* at 78, 79 (Pooler, J., dissenting). According to Judge Pooler's analysis of the majority's opinion, "if an individual subscribes to an Internet E-group and that E-group is determined to have an

illegal purpose, the government has probable cause to obtain a warrant to search the subscriber's home." *Id.* at 78. However, she concludes, "[t]he majority's focus on group probabilities runs counter to the well-settled notion that probable cause must be based on particularized facts," and the corrected affidavit's allegations that the defendant was a subscriber to a website containing child pornography "is simply not enough without something more that indicates that he actually participated in the illegal activities of the group." *Id.* at 81-82.

Two weeks after *Martin I* was decided, a different panel of the Second Circuit was again faced with the exact same issue in *Coreas I*, 419 F.3d 151. The *Coreas I* Court explained that, according to the excised affidavit, all that Coreas did was respond to an invitation to join the Candyman e-group by clicking on a button to add his email address to its role of members, but this "in no way committed him to partaking in any of its various activities, lawful or unlawful." *Id.* at 156. The unanimous panel then stated that "[t]he notion that, by this act of clicking a button, he provided probable cause for the police to enter his private dwelling and rummage through various of his personal effects seems utterly repellant to core purposes of the Fourth Amendment." *Id.* The court further stated their opinion that Coreas broke no law in simply joining the group and that, unless an organization is "wholly illegitimate," membership alone cannot provide probable cause. *Id.* at 156-57.

Despite their own conclusions to the contrary, the *Coreas I* Court explained that they were bound by the *Martin I* Court's decision, which ostensibly held that "a defendant's mere membership in an e-group whose 'primary reason for existence' is to trade in child pornography is enough" to establish probable cause. *Id.* at 157 (citing *Martin I*, 426

F.3d 68). The *Coreas I* panel noted that *Martin I* could arguably be distinguished on the ground that the two websites' homepages and welcome messages were different, but then indicated their belief that the *Martin I* Court "regarded the differences between the websites as immaterial and regarded the Candyman welcome message as explicit enough to warrant an inference of unlawful purpose." *Id.* Ultimately, the *Coreas I* Court concluded that "we believe *Martin* [*I*] itself was wrongly decided. Nonetheless, since the *Martin* [*I*] case was heard first, we are compelled, under established rules of this circuit, to affirm Coreas'[s] conviction." *Id.* at 159.

While the dissension within the same circuit evidenced by the cases discussed directly above should be enough to demonstrate the lack of consensus on this important issue, it must be noted that the confusion and inconsistencies do not end here. In *Martin II*, the court rejected the defendant's petition for rehearing and affirmed their view that probable cause existed in that case because the primary purpose of the website at issue was to facilitate child pornography, "[e]ach member affirmatively joined a collective designed to facilitate the trade of child pornography," and thus it stood to reason that each member's computer was likely to contain evidence, fruits, or instrumentalities of the exchange of child pornography. 426 F.3d at 84-85, 86, 88. However, while affirming its own prior decision, the *Martin II* Court also called into doubt the holding of *Coreas I* by noting in dicta that there might not have been probable cause in *Coreas I* because the website in *Coreas I*, unlike the one in the *Martin* case, did not unequivocally announce that it only contained child pornography. *See id.* at 85-86. The *Martin II* Court disavowed the *Coreas I* Court's "perception" of the *Martin I* Court's holding, noting that "although the Candyman welcome message was not before this panel, we need to clarify that we do not view the differences between the two

welcome messages as 'immaterial.' To the contrary, the girls12-16 welcome message was an integral component of our probable cause determination." *Id.* at 86 (citing *Coreas I*, 419 F.3d at 159). Judge Pooler again dissented in *Martin II*, arguing that there was no probable cause for the same reasons stated in her previous dissent and those stated in the unanimous opinion in *Coreas I*. *Martin II*, 426 F.3d at 89 (Pooler, J., dissenting). She explained that "[s]ince I continue to believe that individualized information, rather than mere membership in an organization whose 'primary purpose' is illegal, is necessary to support a finding of probable cause, the distinction the majority attempts to draw between the welcome messages is unavailing." *Id.* at 90.

Then, based upon the foregoing court decisions, defendant Coreas petitioned for a rehearing. *Coreas II*, 426 F.3d 615. Yet, despite the *Martin II* Court's dicta that the two cases were apparently distinguishable and despite the fact that the *Coreas I* panel had already stated that they believed the *Martin* cases were wrongly decided, the *Coreas II* court reaffirmed its earlier determination that they were bound by *Martin I* and thus denied Coreas's petition for rehearing. *Id.* at 616. The *Coreas II* Court agreed with Judge Pooler's analysis in her *Martin II* dissent that there was no probable cause in either case because, once the erroneous portions of the affidavits were excised, there was no indication that anyone had ever actually downloaded any illegal images. *Id.* However, in an ironic twist, the *Coreas II* Court then invoked the comments in Judge Pooler's *Martin II* dissent–that the two websites were sufficiently similar–in order to reject the *Martin II* majority's dicta that the websites and the welcome pages were distinguishable. *Id.* As the *Coreas II* Court summed up, "we believe that *Martin I* was wrongly decided but that it compels us to affirm Coreas'[s] conviction in this case." *Id.* at 617.

Thus, despite the fact that all three members of the Coreas panel felt there was no probable cause based solely on membership to a website containing child pornography, and despite the fact that one of the three members of the *Martin* panel felt the same way, and despite the fact that the other two members of the *Martin* panel felt there was not necessarily sufficient probable cause in *Coreas*, the denial of both Martin's and Coreas's motions to suppress were upheld due to the utter confusion and chaos inherent in this unresolved issue. Both defendants petitioned for a rehearing *en banc*, which were denied. *See Martin III*, 430 F.3d 73. Once again, Judge Pooler dissented, this time from the denial of the petition. She explicitly "urged the defense attorneys in these cases to seek certiorari" because, in her words, "the precedent set by *Martin* is dangerous and will have far reaching consequences, a concern I know is shared by many of my colleagues." 430 F.3d at 77, 75-76 (Pooler, J., dissenting).

The concern and dissension over this issue expressed by Judge Pooler, however, are not confined to her colleagues within the Second Circuit, as evidenced by the vast array of opinions in other cases which have come down on different sides of this issue. *Compare, e.g.*, *United States v. Strausser*, 247 F.Supp.2d 1135, 1144 (E.D.Mo. 2003) (finding no probable cause to search, in similar case, where excised affidavit reveals nothing more than the subscription to the "Candyman" website containing child pornography, and dismissing the government's position to the contrary as "the equivalent of saying if someone subscribes to a drug legalization organization or newsletter, then there is probable cause to believe that person possesses drugs") *and United States v. Perez*, 247 F.Supp.2d 459, 481 (S.D.N.Y. 2003) (holding, in similar case, that facts in excised affidavit only showed that defendant subscribed to website where unlawful

images of child pornography could be downloaded were not sufficient to permit magistrate to find probable cause to issue search warrant) *with United States v. Froman*, 355 F.3d 882, 890-91 (5th Cir. 2004) (finding probable cause in similar case because magistrate is "entitled to conclude that the overriding reason someone would join this group was to permit him to receive and trade child pornography"); *see also, e.g., United States v. Bailey*, 272 F.Supp.2d 822, 838-39 (D.Neb. 2003) (assuming in a similar case that a warrant to search for child pornography needs some evidence that there has been a delivery of child pornography, but finding probable cause in the instant case because defendant had pornography on the work computer which was searched); *United States v. Kunen*, 323 F.Supp.2d 390, 401-402 (E.D.N.Y.) (noting, in similar case, that association or membership with Internet child pornography website alone is not sufficient to establish probable cause; but finding probable cause in that particular case because false information in affidavits that defendant actually possessed child pornography was not based on intentional or reckless falsehood).[4]

As the various opinions in the cases discussed above clearly demonstrate, the lower courts are in profound disagreement about the issue of whether, absent any individualized averments that a person actually possessed illegal images, membership in a website that contains child pornography in and of itself is sufficient to establish probable cause to issue a search warrant. The vast array of opinions and the vigorous dissents regarding this single issue shows

---

[4] Due to the similarity in the cases, the holdings in *Perez* and *Kunen*, have obviously been called into doubt, if not specifically overruled, by the rulings in the Second Circuit cases of *Martin* and *Coreas*, as discussed *supra*.

that reasonable jurists are in disagreement and that lower courts need clarification. Accordingly, it is respectfully submitted that the Supreme Court needs to address this important and recurring issue and thereby provide guidance to the lower courts on this question. The instant case presents an ideal opportunity for the Supreme Court to authoritatively address this issue because the facts are, for the most part, undisputed, and thus the issue here is focused and direct. As discussed previously, the warrants and their supporting affidavits, as well as the undisputed facts and timeline derived therefrom, merely reveal that Wagers had bought subscriptions to websites that were found at a later date to display child pornography. They did not specifically allege that Wagers had viewed the sites or that he had accessed unlawful content on them at any time.[5] In sum, as one of the affidavits at issue explicitly noted: "the federal agents have no way of ascertaining the actual contents of each website on the various dates customer would have visited the website." (Mimosa Lane Affidavit ¶ 14, Apx. A, p. 51a). Thus, because this case presents the narrow issue of whether membership in a mixed content website–with no specific averments that the defendant actually possessed or downloaded images of child pornography–is sufficient, in and of itself, to establish probable cause under the Fourth

---

[5] Of course, as noted previously, the affidavits did note that Wagers had a previous child pornography conviction. (Mimosa Lane Affidavit ¶ 46, Apx. A, pp. 67a-66a). However, as the Sixth Circuit noted, "Though the affidavit supporting that warrant does take note of his prior offense over less than two full pages, the document is 32 pages long, plus four pages of attachments, and the discussion of his prior offense is not the preponderant support for the application for the warrant." *Wagers II*, 452 F.3d at 541. In other words, "his prior conviction was relevant, though not dispositive," *see id.*, and thus it need not effect the Court's central consideration of the issues presented in this Petition for Certiorari.

Amendment, it would provide an ideal vehicle for the Supreme Court to authoritatively answer this question once and for all.

II. The Issues Presented in this Petition Present an Important, Exceptional, and Recurring Issue of Federal Law Due to the Increased Proliferation and Importance of Computers in Our Society, the Increased Emphasis and Governmental Priority on Prosecution for Internet Child Pornography Cases, and the Fact That Probable Cause and Suppression Issues Remain Unsettled in the Context of Membership with Online Pornography Groups.

As Judge Kleinfeld noted in his dissent in the *Gourde en banc* decision, "the overwhelming importance of the privacy of people's computers makes it essential to assure–even in the this ugly corner of human perversion–probable cause seriously interpreted remain a prerequisite for search warrants." *Gourde en banc*, 440 F.3d at 1084 (Kleinfeld, J., dissenting). For most people, he explained, "their computers are their most private spaces," and "[t]here are just too many secrets on people's computers, most legal, some embarrassing, and some potentially tragic in their implications, for loose liberality in allowing search warrants." *Id.* at 1077. Much of the explanation for this fact that so much private and personal information is contained in our computers undoubtedly lies in the fact that computers and the Internet are so pervasive in our lives and in our society, and that they are becoming more so everyday.[6] The

---

[6] As of March 2006, an estimated 80 million websites existed worldwide, with that number expected to climb exponentially. *See* March 2006 Web Server Survey, at http://news.netcraft.com/archives/2006/03/06/march

Internet–consisting of an almost infinite number of individual websites, each of which allows users with simple software to post text, graphics, images, and moving video into cyberspace–is a unique and wholly new medium of worldwide human communication, which has experienced extraordinary growth. *Reno v. ACLU*, 521 U.S. 844, 849-52 (1997). Since its introduction, the Internet has generated new possibilities for commerce, speech, and the rapid proliferation of information. *See id.*[7] A significant portion of Internet and computer usage is related to pornography.[8]

However, along with this explosion in computer and Internet usage in general, and pornography in particular, there has also been a corresponding increase in the use of computers and the Internet for illicit purposes, including child pornography. Between 2001 and 2005, the number of reports of child pornography sites to the National Center for Missing

---

_2006_web_server_survey.html.

[7] The foundations of the Internet were developed in 1969 through a military program known as ARPANET. *Reno*, 521 U.S. at 849-50. The Internet as we know it today, however, was not introduced until the 1980s and, as the number of personal computer users grew, took on greater prominence in the 1990s. The term "Internet" was officially adopted by the Federal Networking Council in 1995. *See* Barry M. Leiner *et al.*, *A Brief History of the Internet* (Ed. 3.32) at http://www.isoc.org/internet/history/brief.shtml#References (Dec. 10, 2003).

[8] It was estimated that in 2003 approximately 25% of all search engine requests and 8% of all emails are related to pornography, and that 12% of all websites are pornographic. *See* Internet Pornography Statistics: 2003, at http://www.healthymind.com/s-porn-stats.html.

and Exploited Children grew by almost four hundred percent.[9] Accordingly, the United States government has drastically stepped up efforts on several fronts to crack down on the illicit trade in child pornography, including investigating and prosecuting individuals who subscribe to sites containing such material.[10] As such, the issue of whether membership in a website containing child pornography is, in and of itself, sufficient to establish probable cause to issue a search warrant, is undoubtedly one that will continue to arise on a regular, if not increasingly common, basis. And without an authoritative resolution on this profoundly important question of Fourth Amendment law, reasonable jurists in the lower courts will continue to struggle–and continue to disagree–on the answer to this question.

Part of the reason for the ongoing difficulties in resolving this issue is that the regulation of the Internet poses unique challenges for lawmakers and the courts.[11] As this Court has observed, "differences in the characteristics of new media

---

[9] *See* Child Porn Rising on the Web, at http://www.csmonitor.com/2005/0818/p01s01-stct.html.

[10] *See id.*

[11] Additional evidence of the government's attempt to crackdown on the exploitation of children and materials harmful to minors on the Internet include the passage of the Child Protection Act of 1984, 18 U.S.C. § 2251, *et seq.*; the Communications Decency Act of 1996, 47 U.S.C. § 223; the Child Online Protection Act of 1998, 47 U.S.C. § 231; the PROTECT Act of 2003, Pub. L. No. 108-21, 117 Stat. 650; and the most recent amendments to the record keeping requirements in 18 U.S.C. §§ 2257 and 2257A. Although some of these acts have been held unconstitutional, each represents the government's continuing emphasis and priority on the issue of child pornography, and indicates that this is not an issue likely to go away anytime soon.

justify differences in the [constitutional] standards applied to them." *Red Lion Broadcasting Co. v. FCC*, 395 U.S. 367, 386 (1969). Although it may be true that "the Internet does not present a murky new innovation without adequate analogs in the pre-'wired' world," and "[n]o new standard of evidence is necessary for dealing with cases involving the Internet," *see Wagers II*, 452 F.3d at 542; it is also true that

> [i]n this age of increasing government surveillance, lawful and unlawful, and of the retention of all our deeds and thoughts on computers long after we may believe they have been removed, it is important that courts not grow lax in their duty to protect our right to privacy and that they remain vigilant against efforts to weaken our Fourth Amendment protections.

Gourde en banc, 440 F.3d at 1074 (Reinhardt, J., dissenting). As Judge Pooler stated succinctly in her dissenting opinion in *Martin*: "The majority is correct that 'the [I]nternet does not present an exception to established principles of probable cause,' but by relying solely on the fact of membership in a group whose 'primary purpose' is allegedly illegal, that is exactly what they have done in this case." *Martin II*, 426 F.3d at 91 (Pooler, J., dissenting). Whether this legal analysis is right or wrong will likely remain unresolved and a point of contention among the lower courts unless and until this Court clarifies and authoritatively decides the issue.

CONCLUSION

For the foregoing reasons discussed in this Petition, the Court should issue a writ of certiorari to review the decision of the Sixth Circuit affirming the district court's Order denying Mr. Wager's motion to suppress.

This 22nd day of September, 2006.

Respectfully submitted,

H. LOUIS SIRKIN
Counsel of Record
JENNIFER M. KINSLEY
SCOTT RYAN NAZZARINE
Sirkin, Pinales & Schwartz LLP
105 West Fourth Street, Suite 920
Cincinnati, Ohio 45202-2726
Telephone (513) 721-4876
Facsimile (513) 721-0876

Counsel for Petitioners

APPENDIX A

UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

No. 05-5296

[Filed June 27, 2006]

UNITED STATES OF AMERICA,)
Plaintiff-Appellee,)
)
v.)
)
LYMAN WAGERS,)
Defendant-Appellant.)
)

Appeal from the United States District Court
for the Eastern District of Kentucky at Lexington
No. 04-00066
Karl S. Forester, District Judge

Before: BOGGS, Chief Judge; BATCHELDER, Circuit Judge; and WEBER, District Judge.*

* The Honorable Herman J. Weber, United States District Judge for the Southern District of Ohio, sitting by designation.

OPINION

BOGGS, Chief Judge. Lyman Wagers pleaded guilty to receiving and possessing child pornography. On February 11, 2005 he was sentenced to 180 months in prison. The sentence conformed to the 15-year mandatory minimum for second offenders under 18 U.S.C. § 2252(b)(1). Arguing that the three search warrants leading to evidence incriminating him were not supported by probable cause, he appeals the trial court's denial of his motion to suppress evidence seized pursuant to the warrants. *See United States v. Wagers*, 339 F. Supp. 2d 934, 940 & n.1 (E.D. Ky. 2004). We affirm.

I

This is Wagers's second conviction on child pornography charges. He was convicted in 1997 of one count of possession of child pornography and sentenced in the United States District Court for the Eastern District of Kentucky to 366 days in prison, plus three years of supervised release. In the case now before us, Wagers, a 57-year-old erstwhile lawyer and C.P.A., pleaded guilty to one count of conspiracy to receive child pornography, nineteen counts of receiving child pornography, and one count of possession of child pornography. The terms of his guilty plea allowed him to appeal the conviction on the grounds that the search warrants used in the investigation were not supported by probable cause.

A Homeland Security sting operation led to Wagers's arrest. From March to August 2003, federal agents purchased subscriptions to and visited websites available at redlagoon.com, video2000.com, and darkfeeling.com. While visiting these sites, the agents found images of child pornography. They obtained records from the billing services

of these sites. These records revealed that Wagers had purchased subscriptions to redlagoon.com on June 30, 2002; to video2000.com on March 22, 2003 and again on June 3, 2003; and to darkfeeling.com on April 15, 2003. Though the lengths of Wagers's subscriptions are not clear from the record, based on the prices he paid for his subscriptions, as compared to the prices the agents paid for one-month subscriptions, it appears that each of Wagers's subscriptions was for between one and two months of membership. This inference has been offered by Wagers and is not contested by the government. The agents who examined the websites did so by purchasing one-month subscriptions on March 26, 2003, August 1, 2003, and July 21, 2003, respectively.

On April 5, 2004, federal agents executed a search warrant at the home of Lyman Wagers ("Mimosa Lane" or "home"). After finding child pornography on Wagers's home computer, agents swore out another affidavit for his office. On April 7, 2004, agents obtained a separate warrant for his office ("Harrodsburg Rd." or "office"). The same day, he was arrested for possession of child pornography. The following day, agents obtained a third search warrant, directed to America Online, the company supporting Wagers's email account ("AOL" or "email"). Wagers's guilty plea and conviction are based on images found on his home computer, at least some of which, he concedes, were transmitted via his American Online account.

The home and office affidavits were both more than thirty pages long and quite detailed. The AOL affidavit is seven pages and less detailed, but it states that agents had connected Wagers's AOL email address to his home address and to the purchase of subscription memberships to all of the websites containing offending material. It further states that the affiant's "experience and training" lead him to believe that

Wagers uses his AOL account to "order, arrange for the payment of, and arrange for the receipt of child pornography . . . ." *Id.* at 162. The warrants and their supporting affidavits alleged that Wagers had bought subscriptions to websites that were found at a later date to display child pornography. They did not specifically allege that Wagers had viewed the sites or that he had accessed unlawful content on them.

A federal grand jury indicted Wagers on May 6, 2004. He moved to suppress the evidence seized at his home and office. The district court denied the motion without a hearing. Wagers pleaded guilty to all counts, conditioning the plea on his right to appeal the ruling on the motion to suppress.

The district court sentenced Wagers to 180 months in prison on February 11, 2005. The guidelines range was 97 to 121 months, but the sentence conformed to the 15-year mandatory minimum for second offenders required by 18 U.S.C. § 2252(b)(1).

Wagers timely appealed his conviction, challenging the district court's denial of his motion to suppress.

II

This court reviews a district court's factual findings supporting its denial of a motion to suppress for clear error. It reviews *de novo* the district court's determination as to the reasonableness of the search as a question of law. *United States v. Carpenter*, 360 F.3d 591, 594 (6th Cir. 2004) (en banc); *United States v. Harris*, 255 F.3d 288, 291-92 (6th Cir. 2001). The "appellate court must consider the evidence in the light most favorable to the government" when reviewing a denial of a motion to suppress. *United States v.*

Herndon, 393 F.3d 665, 667 (6th Cir. 2005) (quoting *United States v. Erwin*, 155 F.3d 818, 822 (6th Cir. 1998) (en banc)). "Probable cause exists where there is a fair probability, given the totality of the circumstances, that contraband or evidence of a crime will be found in a particular place." *United States v. Helton*, 314 F.3d 812, 819 (6th Cir. 2003) (quoting *United States v. Davidson*, 936 F.2d 856, 859 (6th Cir. 1991)).

III

Wagers's first major argument is that the affidavits were not supported by probable cause for three reasons:

1) the affidavits supporting the search warrants did not allege that he had owned website memberships at a time when illegal images were mounted on the sites or that he had accessed the sites during the times when illegal images were available;

2) the affidavits do not adequately connect the illicit activity to his home, office, or AOL account; and

3) the affidavit for the home warrant improperly relied on the fact of Wagers's prior conviction.

In this section, we address each component of this argument in turn. In section IV of this opinion we address the second major argument of Wagers's appeal.

Wagers notes that the agents' subscriptions post-dated the expiration of all but possibly one of his own subscriptions. He argues that the affidavits supporting the search warrants merely infer that there were unlawful images on those sites at the time of his earlier subscriptions.

To assess how much of an inference was made in issuing the search warrants, it is useful to observe that roughly five months elapsed between the end of Wagers's subscription to redlagoon.com and the commencement of the agents' subscription. Approximately one month passed before their subscriptions to darkfeeling.com. And it is possible that only a few days elapsed between the end of Wagers's second subscription to video2000.com and the government's. Indeed, if Wagers's subscription was for two months (which, according to his own brief's uncontested calculation of "between one and two months," is possible), there would be a short overlap between the end of his second subscription and the government's subscription. Whether or not there was an actual overlap between subscriptions, an inference based on the difference of a few days-in the case of video2000.com-or of roughly 30 days-in the case of darkfeeling.com-is not very hard to make, even setting aside the perhaps more tenuous inference based on research on redlagoon.com that was five months after Wagers's known use.

Wagers claims in his brief (Appellant's Brief, 12) that these three websites contained both legal and illegal images. The government claims this assertion is false. (Appellee's Brief, 12) Wagers does not offer clear support for his statement in the record. Neither, for that matter, does the United States. The government points only to two printouts in the Joint Appendix submitted to this court, of the homepages of darkfeeling.com and redlagoon.com, both of which announce that *all* models featured on the sites are "14 or younger." (JA 195-96) These homepage reproductions are highly suggestive but not conclusive. Advertisers have been known to mislead before. Wagers rebuts, moreover, that the affidavits never state that the sites offer exclusively illegal content. Appellant's Reply Brief, 7. Neither party's view is definitive. But the district court was correct in concluding that

this question is not dispositive. Probable cause to search for illicit pornography in Wagers's home, office, and email account existed even without a statement that these three websites contained only illegal images. *See* 339 F. Supp. 2d at 940 & n.1 The district court's conclusion is especially strong in light of the temporal analysis: based on the proximity in time between their subscriptions and his, the agents were justified in averring the essential similarity of the websites at the time Wagers had subscribed to them to the sites as they appeared during the sting operation's subscriptions.

Wagers argues that the affidavits do not connect the alleged crime to the places searched. For a search warrant to be valid, the place to be searched must be connected to the crime alleged. *E.g.*, *United States v. Laughton*, 409 F.3d 744 (6th Cir. 2005). Wagers does not dispute that he lived at 3813 Mimosa Lane, for which the first warrant issued. However, he does contend that "there is nothing in the affidavit connecting the residence to the alleged child pornography offenses." Appellant's Brief, 14. He offers two feeble pieces of support for this argument. First, he notes that he did not get Internet access at this residence until October 9, 2002, months after his subscription to redlagoon.com expired. However, his subscriptions to the other two websites post-date this Internet access.

Second, he notes that his subscriptions to video2000.com and darkfeeling.com were made on a checking card with a billing address of 1608 Harrodsburg Rd. in Lexington. Therefore, he argues, his subscriptions were connected only to his business office, not to his home, even though his home was the subject of the first warrant. However, the affidavit sworn by Homeland Security Special Agent Sean Lichner in support of the April 5, 2005 search warrant of the Mimosa

Lane home notes specifically that the investigation into the subscription records of the three websites revealed that a subscriber's email address "Spike20004U@aol.com" was connected to 1608 Harrodsburg Rd. and 3813 Mimosa Lane, both in Lexington, Kentucky. The affidavit also avers that two credit card numbers and a phone number associated with the Mimosa Lane address were obtained from the websites' billing service provider, and that these data were soon connected to the name Lyman Wagers.

In addition, the affidavit avers that the investigation revealed that Wagers used Insight Communications as his home Internet service.[1] *Id.* at 99. It further avers that an IP address assigned by Insight to Wagers was used to purchase both memberships at video2000.com and the membership at darkfeeling.com. *Ibid.* Because this IP address was assigned by Insight, and because it appears from the wording of the affidavit that Wagers used Insight at his home but not his office, his home would be well within the ambit of a properly issued search warrant. Even if the home were only one of two locations-home and office-served by Insight, there would be sufficient evidence to support probable cause. Given the specificity of the investigation's results and the content of the affidavit, the warrant was valid.

Wagers cites *United States v. Savoca*, 761 F.2d 292, 297 (6th Cir. 1983), for the proposition that the "existence of probable cause to believe a suspect is guilty of a crime does not create probable cause to search that individual's residence

---

[1] The affidavit notes that Wagers uses Insight as the Internet provider for his home. It also notes that Insight had his office address for billing purposes. However, it appears from the wording of the affidavit that Wagers did not use Insight at his office, but only at his home.

without independent evidence establishing a nexus between the place and the crime." Appellant's Brief, 15. *Savoca* did not involve a home, but a motel room, a location subject to a lesser expectation of privacy. Second, and more importantly, we criticized the affidavit in that case as "only tenuously connect[ing] the place to be searched with two persons for whom arrest warrants were outstanding," for "fail[ing] to describe the relationship of the persons to the premises," and because it "did not state, for example, whether the location to be searched was a permanent residence, a transient lodging, or a third party's residence which the two named persons were merely visiting." The affidavit stated only that "both suspects 'were seen' in the motel room on two occasions." *Id.* at 297 and n.8. The affidavit in our case is much more specific.

It is true that, in *United States v. Helton*, 314 F.3d 812, 821 (6th Cir. 2003), this court held that, even where police investigations revealed that a defendant was closely connected to possession of narcotics, a search warrant for his home was invalid without any evidence linking that residence to the drug trade. However, that case is easily distinguished. First, part of the affidavit was based on an anonymous tipster, which the court reasonably found to have been insufficiently reliable to form the basis of probable cause. *Id.* at 821-22. Second, part of the affidavit was based on a confidential informant's allegation, much of which pointed to a home other than the defendant's. *Id.* at 821. No such affirmative evidence, pointing to places other than Wagers's home or business, appears here. Third, the remainder of the affidavit was based on the placing of three phone calls per month from the defendant's home telephone to the number of a known drug trafficker. The evidence in our case connecting the defendant, his computer, his IP address, and his home to the offense is considerably stronger, particularly where the criminal activity

(viewing child pornography) is much more tied to a place of privacy, seclusion, and high-speed Internet connectivity (e.g. a home or office) than the storing of drugs (which can take place in a car, a ditch, a hole in the ground, etc.).

Our opinion today is consistent with the views of our sister circuits. The Second and Fifth Circuits, for example, have noted that evidence that a person has visited or subscribed to websites containing child pornography supports the conclusion that he has likely downloaded, kept, and otherwise possessed the material. *United States v. Martin*, 418 F.3d 148, 157 (2d Cir. 2005); *United States v. Froman*, 355 F.3d 882, 890-91 (5th Cir. 2004).

As to the third warrant in his case, the one served on AOL, Wagers notes that the affidavit sworn in support of this warrant observes mostly that he subscribed to and visited websites. The only reference to email in the affidavit is the affiant's stated "belie[f] that Wagers uses the spike20004U@aol.com email account to order, arrange for the payment of, and arrange for the receipt of child pornography." (JA 162, quoted at Appellant's Brief, 17) Wagers also used an IP address furnished by AOL to sign up for at least one of his subscriptions. An offender without relatively sophisticated knowledge of transmittal or downloading technology might reasonably be expected to use email to send and receive pornographic images or at least web links to them. Probable cause does require a sufficient nexus between the location to be searched and the evidence sought. *United States v. McLevain*, 310 F.3d 434, 439 (6th Cir. 2002). This court, in *United States v. Schultz*, 14 F.3d 1093 (6th Cir. 1994), declined to find such a nexus-and held that the avowed training and experience of law enforcement-affiants failed to subsitute for it-where police suspected a defendant of drug offenses and therefore sought to search his

safety deposit box. However, the nexus between an AOL email account and Internet-accessed child pornography, especially where some of that access has been through AOL IP addresses, is much more obvious than the connection between drug trafficking and safety deposit boxes.

Wagers's final argument on the warrant's sufficiency is that the affidavit for the home warrant "relies heavily upon the fact that Wagers had a previous child pornography conviction." (Appellant's Brief, 15) Though the affidavit supporting that warrant does take note of his prior offense over less than two full pages, the document is 32 pages long, plus four pages of attachments, and the discussion of his prior offense is not the preponderant support for the application for the warrant. Implying that a prior conviction cannot properly raise an inference of later criminal activity, even for an identical or nearly identical offense, Wagers argues that an "individual's criminal history . . . is not the appropriate focus for a search warrant affidavit." Appellant's Brief, 16. Wagers's only citation of law for this proposition is *Mays v. City of Dayton*, 134 F.3d 809, 814 (6th Cir. 1998), stating that "[s]earch warrants are directed not at persons, but at specific locations where there is probable cause to believe the instrumentalities or evidence of crimes will be found." This case does not help Wagers's larger implied argument here, to the effect that search warrants based in part on prior convictions are presumptively invalid. The test for probable cause, as the Supreme Court affirmed very recently in *United States v. Grubbs*, 126 S. Ct. 1494, 164 L. Ed. 2d 195 (2006), is whether "'there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" *Grubbs* at 1499 (quoting *Illinois v. Gates*, 462 U.S. 213, 238, 103 S. Ct. 2317, 76 L. Ed. 2d 527 (1983)). The application of this test is not fettered by the presumption of innocence embodied in the test for conviction. Instead, a "person of

reasonable caution" would take into account predelictions revealed by past crimes or convictions as part of the inquiry into probable cause. *See, e.g., United States v. Blanton*, 520 F.2d 907, 912 (6th Cir. 1975) (finding probable cause to search defendant's car where the arresting officer was reliably informed that the car trunk contained a machine gun and money, where the officer knew that the defendant had extensive use of the car, and where the officer personally knew the defendant well enough to know of his "past criminal record"). Wagers's prior conviction for possession of child pornography followed the seizure of illegal images on both his home and his office computers. When, in our case, the Homeland Security agents uncovered evidence of Wagers's connection to the websites carrying child pornography, his prior conviction was relevant, though not dispositive. Given the requirements of seclusion and a high-speed Internet connection, a home and office search warrant is supported by probable cause under these circumstances. For this reason, and for the several reasons already adduced *supra*, the district court did not abuse its discretion in denying a motion to suppress evidence gathered pursuant to a search warrant for Wagers's home and office.

IV

Wagers's secondary point is that the Internet is an "ever-changing global method of communication" that "heighten[s]" the "importance of the probable cause requirement." (Appellant's Brief, 8) Some websites contain both lawful images and unlawful images. He argues that the Internet presents too many opportunities for search warrants to be issued where innocent activity and criminal activity may be easily confused or accidentally mixed (*e.g.*, by visiting websites containing legal and illegal images). His argument here seems to be that the Internet is a new and different

entity, and that such an entity should be analyzed cautiously by law enforcement and courts. A lurking point, though Wagers never states it explicitly (most likely because he was caught red-handed with at least six hundred graphic and disturbing images of children having-or being forced to have-sex), is that the Internet may present too many opportunities for a search warrant to be issued where innocent activity (viewing lawful pornography) and criminal activity (viewing unlawful pornography) may be easily confused or accidentally mixed, as by visiting websites that may contain lawful and unlawful pornography. His contention implies rejection of the common law's capacity to handle significant innovation and novelty.[2]

The tools available to us are adequate to the task of helping us understand the risks posed to Fourth Amendment rights by the type of law enforcement we see in the appeal before us. As it applies to the facts of Wagers's case, the Internet does not present a murky new innovation without adequate analogs in the pre-"wired" world. In essence, Wagers's Internet argument is just a variation of the "simply in the wrong place at the wrong time" refrain. This type of argument is not infrequently put forward in other contexts, for example by persons attacking search warrants based, in part,

---

[2] This capacity has, at times, been considered perfect. *See* Joseph H. Beale, *A Treatise on the Conflict of Laws* § 3.2, 4.12 (1935) (describing the common law as a seamless web of interlocking principles which, properly applied, can fully accommodate intelligent analysis of a case arising from commerce with any technological invention, including, illustratively, the streetcars of mid-nineteenth century Boston, which Chief Justice Lemuel Shaw deftly analyzed using existing common law analysis in *Commonwealth v. Temple*, 80 Mass. (14 Gray) 69, 74, 14 Gray 69 (1859)).

on their presence in a shady part of town, near the scene of a murder, or any number of locales or factors that could also have an innocent explanation. Indeed, it is a commonplace part of judging attacks on convictions as well as warrants (with their lower standard of proof), that the law can properly judge evidence that could be consistent with innocence as well as guilt, and that our system can make a valid determination as to which obtains in a particular fact pattern. It is well established in this court that "the probable cause requirement does not require that every contrary hypothesis be excluded." *United States v. Alfano*, 838 F.2d 158, 162 (6th Cir. 1988). No new standard of evidence is necessary for dealing with cases involving the Internet. All that is required is a consistent application of our existing approaches to possibly ambiguous evidence.

To press his argument that the Internet poses novel risks to constitutional law enforcement, Wagers relies heavily on the Ninth Circuit's recent decision in *United States v. Gourde*, 382 F.3d 1003 (9th Cir. 2004). In that case, the defendant was arrested following the execution of a search warrant based on an affidavit that alleged that he subscribed to a website that contained both lawful and child pornography but silent on the question whether he had actually used the site and/or accessed its content. *Id.* at 1007. The Ninth Circuit panel invalidated the search warrant as supported by insufficient information to furnish probable cause. The court demanded particularized information that the defendant had viewed illegal images. *Id* . at 1013.

His reliance on *Gourde* is flawed for three compelling reasons. First, Gourde appears to have had no prior convictions for child pornography. Wagers does. Following questioning pursuant to his 1997 arrest, the FBI learned that Wagers had transmitted "many more than [four]" images via

his AOL "internet connection" (though it is unclear whether this transmittal refers to "email" or just his means of "surfing") in the years preceding that arrest.[3] Second, the affidavit supporting the search warrant in *Gourde* expressly noted that the website visited in that case, Lolitgurls.com, featured images of "adult pornography, child pornography, and child erotica." (Affidavit of David J. Moriguchi, filed January 29, 2003, page 3) The affidavits supporting the search warrants in our case note only that the websites visited by Wagers featured illegal images. They are silent on whether these sites also included legal pornography. Third, the *Gourde* ruling was substantially overturned en banc. *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006) (en banc). The en banc court held that probable cause did exist in the case.

V

Because the district court properly denied Wagers's motion to suppress evidence, we **AFFIRM** his conviction.

---

[3] For precision and completeness, it bears noting that the defendant admitted to having "transmitted many more than that number," where "that number" equaled "four."

APPENDIX B

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY

Case Number: LEXINGTON CR. 04-66-SS - KSF

USM Number: 06359-032

[Filed February 11, 2005]

UNITED STATES OF AMERICA	)
	)
v.	)
	)
LYMAN E. WAGERS, JR.	)
	)

JUDGMENT IN A CRIMINAL CASE

THE DEFENDANT:

X pleaded guilty to count(s) 1ss - 21ss

The defendant is adjudicated guilty of these offenses:

Title & Section	Nature of Offense
18 U.S.C. 2252(b)(1)	Conspiracy to receive child pornography
Offense Ended	**Count**
3/14/04	1ss
Title & Section	**Nature of Offense**
18 U.S.C. 2252(a)(2)	Receipt of child pornography
Offense Ended	**Count**
3/14/04	2ss - 20ss
Title & Section	**Nature of Offense**
18 U.S.C. 2252(a)(4)(B)	Possession of child pornography
Offense Ended	**Count**
4/7/04	21ss

The defendant is sentenced as provided in pages 2 through 6 of this judgment. The sentence is imposed pursuant to 18 U.S.C. § 3553(a) and the Sentencing Reform Act of 1984 as amended or modified by the Supreme Court's January 12, 2005, decision in United States v. Booker and United States v. Fanfan.

X Count(s) Original & 1st superseding indictment X are dismissed on the motion of the United States.

It is ordered that the defendant must notify the United States attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this

judgment are fully paid. If ordered to pay restitution, the defendant must notify the court and United States attorney of material changes in economic circumstances.

February 11, 2005
Date of Imposition of Judgment

/s/
Signature of Judge

KARL S. FORESTER, CHIEF JUDGE
Name and Title of Judge

February 11, 2005
Date

IMPRISONMENT

The defendant is hereby committed to the custody of the United States Bureau of Prisons to be imprisoned for a total term of:

180 months on each count to run concurrently, for a total term of 180 months.

X The defendant shall surrender for service of sentence at the institution designated by the Bureau of Prisons:

X before 2 p.m. on 3/14/05.

SUPERVISED RELEASE

Upon release from imprisonment, the defendant shall be on supervised release for a term of:

Life on each of Counts 1ss and 12ss through 21ss and terms of three (3) years on each of Counts 2ss through 11ss, all such terms to run concurrently.

The defendant must report to the probation office in the district to which the defendant is released within 72 hours of release from the custody of the Bureau of Prisons.

The defendant shall not commit another federal, state or local crime.

The defendant shall not unlawfully possess a controlled substance. The defendant shall refrain from any unlawful use of a controlled substance. The defendant shall submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter, as determined by the court.

X The defendant shall not possess a firearm, destructive device, or any other dangerous weapon. (Check, if applicable.)

X The defendant shall register with the state sex offender registration agency in the state where the defendant resides, works, or is a student, as directed by the probation officer. (Check, if applicable.)

If this judgment imposes a fine or restitution, it is a condition of supervised release that the defendant pay in

accordance with the Schedule of Payments sheet of this judgment.

The defendant must comply with the standard conditions that have been adopted by this court as well as with any additional conditions on the attached page.

STANDARD CONDITIONS OF SUPERVISION

1) the defendant shall not leave the judicial district without the permission of the court or probation officer;

2) the defendant shall report to the probation officer and shall submit a truthful and complete written report within the first five days of each month;

3) the defendant shall answer truthfully all inquiries by the probation officer and follow the instructions of the probation officer;

4) the defendant shall support his or her dependants and meet other family responsibilities;

5) the defendant shall work regularly at a lawful occupation, unless excused by the probation officer for schooling, training, or other acceptable reasons;

6) the defendant shall notify the probation officer at least ten days prior to any change in residence or employment;

7) the defendant shall refrain from excessive use of alcohol and shall not purchase, possess, use, distribute, or administer any controlled substance or any paraphernalia related to any controlled substances, except as prescribed by a physician;

8) the defendant shall not frequent places where controlled substances are illegally sold, used, distributed, or administered;

9) the defendant shall not associate with any persons engaged in criminal activity and shall not associate with any person convicted of a felony, unless granted permission to do so by the probation officer;

10) the defendant shall permit a probation officer to visit him or her at any time at home or elsewhere and shall permit confiscation of any contraband observed in plain view of the probation officer;

11) the defendant shall notify the probation officer within seventy-two hours of being arrested or questioned by a law enforcement officer;

12) the defendant shall not enter into any agreement to act as an informer or a special agent of a law enforcement agency without the permission of the court; and

13) as directed by the probation officer, the defendant shall notify third parties of risks that may be occasioned by the defendant's criminal record or personal history, or characteristics and shall permit the probation officer to make such notifications and to confirm the defendant's compliance with such notification requirement.

SPECIAL CONDITIONS OF SUPERVISION

The defendant shall not possess a firearm, destructive device, or dangerous weapon.

The defendant shall be required to participate in the sex offender treatment program as adopted by the Courts of the Eastern District of Kentucky. The defendant shall pay the costs of any/all polygraph examinations.

The defendant shall participate in a substance abuse treatment program and shall submit to periodic drug and alcohol testing at the direction and discretion of the probation officer during the term of supervision.

Pursuant to Public Law 108-405, Revised DNA Collection Requirements Under the Justice for All Act of 2004, the defendant shall submit to DNA collection if the offense of conviction is a felony.

CRIMINAL MONETARY PENALTIES

The defendant must pay the total criminal monetary penalties under the schedule of payments on Sheet 6.

	Assessment	Fine	Restitution
TOTALS	$ 2,100.00	$	$

If the defendant makes a partial payment, each payee shall receive an approximately proportioned payment, unless specified otherwise in the priority order or percentage payment column below. However, pursuant to 18 U.S.C. § 3664(i), all nonfederal victims must be paid before the United States is paid.

SCHEDULE OF PAYMENTS

Having assessed the defendant's ability to pay, payment of the total criminal monetary penalties are due as follows:

A X Lump sum payment of $2,100.00 due immediately,

F X Special instructions regarding the payment of criminal monetary penalties:

Criminal monetary penalties are payable to:
Clerk, U. S. District Court
Eastern District of Kentucky
Post Office Box 3074
Lexington, KY 40588-3074

Unless the court has expressly ordered otherwise, if this judgment imposes imprisonment, payment of criminal monetary penalties is due during imprisonment. All criminal monetary penalties, except those payments made through the Federal Bureau of Prisons' Inmate Financial Responsibility Program, are made to the clerk of the court.

The defendant shall receive credit for all payments previously made toward any criminal monetary penalties imposed.

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) fine principal, (5) fine interest, (6) community restitution, (7) penalties, and (8) costs, including cost of prosecution and court costs.

APPENDIX C

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF KENTUCKY

Criminal Action No. 04-66-S

[Filed October 12, 2004]

UNITED STATES OF AMERICA,)
Plaintiff,)
)
v.)
)
LYMAN WAGERS, JR.,)
Defendant.)
)

KARL S. FORESTER, CHIEF JUDGE

MEMORANDUM OPINION AND ORDER

This matter is before the Court for consideration of the Defendant Lyman Wagers, Jr.'s (hereafter, the "Defendant" or "Wagers") Motion to Suppress certain evidence discovered pursuant to the execution of three (3) search warrants at his residence, his business and America On-Line's corporate headquarters regarding his account [DE # 30]. The United States has filed a Response to the Motion to Suppress [DE # 34], the Defendant replied [DE # 36], and the government submitted a Sur-Reply. [DE # 37] Concurrent with his reply,

Wagers also filed a Motion for leave to place evidence in the record absent a stipulation [DE # 36], to which the United States responded. [DE # 37] Accordingly, the motions are now ripe for adjudication.

I. BACKGROUND

Previously, the United States submitted three (3) Applications and Affidavits for Search Warrants regarding an investigation into Mr. Wagers' alleged criminal wrongdoings involving child pornography. Specifically, the United States sought to search the residential and business premises of Mr. Wagers at 3818 Mimosa Lane, Lexington, Kentucky and 1608 Harrodsburg Road, Lexington, Kentucky on April 5 and 8, 2004, respectively. [*See* April 5, 2004, Application and Affidavit For Search Warrant, hereafter the "April 5th Affidavit", and April 8, 2004 Application and Affidavit For Search Warrant, hereafter the "April 8th Affidavit".] The United States also filed an application for search warrant for searching records involving Mr. Wagers at America On-Line's (AOL) headquarters in Dulles, Virginia, on April 8th. [See the April 8, 2004, Application and Affidavit For Search Warrant of AOL Headquarters, hereafter the "AOL Affidavit".] Based on these applications and affidavits, and after finding probable cause had been established, Magistrate Judge James B. Todd signed each application and issued search warrants on the corresponding dates the warrants were submitted.

Wagers now challenges the sufficiency of those affidavits in the instant Motion to Suppress. Through his motion, Wagers argues that the evidence seized pursuant to three (3) search warrants should be suppressed because: (1) they do not create probable cause to believe that Mr. Wagers committed any crime; and (2) they do not create probable

cause to believe that instrumentalities or evidence of a crime would have been found at the premises to be searched. For the reasons stated herein, Wagers' Motion to Suppress will be DENIED.

II. LEGAL STANDARD

The Fourth Amendment to the United States Constitution provides:

> No Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the places to be searched, and the person or things to be seized.

U.S. Const., Amend. IV. Wagers does not challenge the "particularity" of the affidavits; rather, he contests the sufficiency of the "probable cause" for the issuance of said search warrants.

To be sufficient, the affidavits must establish probable cause to believe that evidence of the alleged crimes would be present at the three premises searched. *United States v. Davidson*, 936 F.2d 856, 859 (6th Cir. 1991). Probable cause is defined as "reasonable grounds for belief, supported by less than prima facie proof but more than mere suspicion," *United States v. Bennett*, 905 F.2d 931, 934 (6th Cir.1990), and is said to exist "when there is a 'fair probability,' given the totality of the circumstances, that contraband or evidence of a crime will be found in a particular place." *Davidson*, 936 F.2d at 859; *see also, e.g., United States v. Johnson*, 351 F.3d 254, 258 (6th Cir.2003). In reviewing the sufficiency of a search warrant affidavit, the "magistrate's determination of probable cause is afforded *great deference*," and should only be reversed if arbitrarily made. *United States v. Greene*, 250

F.3d 471, 478 (6th Cir.2001)(emphasis added); *United States v. Finch*, 998 F.2d 349, 352 (6th Cir. 1993). To this end, "review of an affidavit and search warrant should rely on a 'totality of the circumstances' determination, rather than a line-by-line scrutiny." *Greene*, 250 F.3d at 479. In other words, the magistrate judge's responsibility in examining the challenged search warrant is "simply to make a *practical, common sense decision* whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238, 103 S. Ct. 2317, 76 L. Ed. 2d 527 (1983) (emphasis added).

"It is well settled that in seeking suppression of evidence the burden of proof is upon the defendant to display a violation of some constitutional or statutory right justifying suppression." *United States v. Feldman*, 606 F.2d 673, 679 n. 11 (6th Cir.1979). "When reviewing the denial of a motion to suppress evidence, we must consider the evidence in the light most favorable to the government." *United States v. Garza*, 10 F.3d 1241, 1245 (5th Cir.1993). The standard of review for determining the sufficiency of the affidavit "is whether the magistrate had a substantial basis for finding that the affidavit established probable cause to believe that the evidence would be found at the place cited." *United States v. Davidson*, 936 F.2d 856, 859 (6th Cir.1991). *See U.S. v. Rodriguez-Suazo*, 346 F.3d 637, 643 (6th Cir.2003).

III. ANALYSIS

A. The Affidavits In General

Prior to the initiation of the instant criminal action, as ascertained from the averments contained in the supporting

affidavits, a number of police and investigatory agencies, including the United States Attorney's Office for the District of New Jersey, the United States Department of Justice's Child Exploitation and Obscenity Section, the New Jersey offices of the ICE, Internal Revenue Service, Criminal Investigations Division, the United States Postal Inspection Service, and the Federal Bureau of Investigations, conducted a joint investigation into the business known as Regpay, a third party billing and credit card aggregating company. [*See* April 5th Affidavit, ¶¶ 10-23; April 8th Affidavit, ¶¶ 10-23; AOL Affidavit, pp. 1-2.] Through this independent investigation, the foregoing agencies discovered that Regpay was conspiring with other website operators to commercially distribute child pornography by providing those other site operators with billing and credit card aggregating services. Id. The investigation also revealed that Regpay received a percentage of the website operator's revenues and also operated its own website(s) that sold child pornography. [*See* April 5th Affidavit, ¶¶ 10-12; April 8th Affidavit, ¶¶ 10-12.]

The agencies' undercover agents purchased a membership and visited several sites serviced by Regpay. *Id.* Between February and September 2003, the agents verified that at least 21 websites that were serviced by Regpay were still accessible, active and contained child pornography. Critically, the instant affiant admitted that the agents had no way of ascertaining the actual contents of each website on the various dates customers actually visited the websites in March, July and August 2003. [*See* April 5th Affidavit, ¶ 14; April 8th Affidavit, ¶ 14.] Yet, the agents were able to verify that, on the dates they visited the various sites, the sites contained child pornography, as defined by federal law. *Id.* The affidavits contain detailed explanations of the process used by federal agents to secure the computers and databases used by Regpay and Iserve, as well as how the agents retrieved

member data from those databases subsequent to the seizure of the various suspect computer equipment. [*See* April 5th Affidavit, ¶¶ 10-23; April 8th Affidavit, ¶¶ 10-23.] Wagers does not contest the factual accuracy of the underlying investigation.

Importantly, as will be demonstrated herein, the affidavits clearly attest that "there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, as set forth [in the affidavit] will be located at the SUBJECT PREMISES." [*See* April 5th Affidavit, ¶ 7; April 8th Affidavit, ¶ 7. *See also* AOL Affidavit, p. 6 (stating probable cause to believe that Wagers used his AOL account to receive child pornography.] The financial records from both Regpay, or one of its associated companies like Iserve, and Mr. Wagers' credit/bank card companies, American Express and Visa/Bank One, obtained by subpoena, confirm purchases of subscriptions by Wagers to three (3) different websites that contain(ed) child pornography. [*See* April 5th Affidavit, ¶¶ 30-31, 36-41; April 8th Affidavit, ¶¶ 30-31, 36-41.] Records from Insight Communications, Wagers' internet broadband provider, also obtained by subpoena, confirm that three (3) websites containing child pornography were accessed from the IP address assigned by Insight to Mr. Wagers. [*See* April 5th Affidavit, ¶¶ 32-35; April 8th Affidavit, ¶¶ 32-35; AOL Affidavit, p. 4-6.] Further, the AOL user name purchased and used by Wagers, Spike20004u@aol.com, was paid for with the same Visa/Bank One check card used to pay for access to websites containing child pornography. [*See* April 5th Affidavit, ¶¶ 28-31; April 8th Affidavit, ¶¶ 28-31; AOL Affidavit, pp. 3-4.] That card is registered to Mr. Wagers.

Mr. Wagers' subscriptions to the three sites at issue apparently expired prior to the undercover agents accessing

and viewing each subject website. [*See* DE # 30, pp. 2-3, 5-6.] Specifically, the agents viewed the "Red Lagoon" website 8 months after Mr. Wagers' subscription expired; the agents accessed the "Video-2000" site a month after Wager's subscription expired; and the agents viewed the "Dark Feeling" website about 2 months after his subscription expired. Id. Wagers makes much ado about the fact that the affidavit does not, however, state that the suspect websites contained pornographic material for the periods of time during which Wagers held subscriptions to these sites. Nevertheless, as explained below, this failure is neither dispositive nor affective of the instant motion, especially considering case law regarding the retention of child pornography on people's computers.

Turning to Wagers' motion, the Defendant points out that the affidavits at issue are

> devoid of any proof that child pornography was offered on these websites when Mr. Wagers held his subscriptions, devoid of any information that Mr. Wagers utilized these websites after purchasing his subscriptions, devoid of any information that if he did use them, he viewed illegal rather than legal portions of the websites, devoid of any information that Mr. Wagers downloaded anything from these websites, and devoid of any information that, if downloading was performed, the fruits of such downloading were still in the possession of Mr. Wagers at the subject premises.

[DE # 30, pp. 2-3] Primarily, Wagers argues that the agents, as evidenced by the affidavits, had no evidence that the subject websites contained child pornography when he was a member of the subject websites or that he accessed, viewed

images on or downloaded anything from those sites. He also contends that the affidavits are incorrect insofar as they state that the "customer transaction records indicate that four of the member-only sites purchased by [him] permitted electronic access to child pornography," when there is no such proof that they did so at the time of his subscriptions. However, Wagers attacks what he *claims* the affidavits lack rather than focusing on what they actually contain and assert. He admits that the investigation correctly ascertained that he had purchased subscriptions to the three suspect websites through Regpay's and/or Iserve's billing service.

Wagers also argues that the affidavits require the agents and magistrate judge to stack inferences in finding "probable cause." Specifically, he relies upon a recent Ninth Circuit opinion, *United States v. Gourde*, 382 F.3d 1003, 2004 WL 1945331 (9th Cir. 2004). That case, however, is distinguishable on the facts. First, it is not binding precedent in this Circuit. Second, the government agents in that case could have, but did not, track the defendant's actual usage of the suspect child pornographic website. Critically, and perhaps most importantly, the suspect affidavit in *Gourde* did *not* contain any allegations that Gourde had actually downloaded, received, transmitted or otherwise possessed child pornography and did not attest to the dates of the various images accessed by the agents. *Id.* at --. As discussed below, and set forth in the affidavit in the case *sub judice,* the attesting officer undoubtedly averred that probable cause existed for finding images of child pornography in various forms. [Affidavit, ¶ 53]

B. Mimosa Lane and Harrodsburg Road Affidavits

Wagers argues that the April 5th Affidavit sets forth no factual allegations connecting his Mimosa Lane residence to

the website subscriptions. He states that the Red Lagoon subscription, purchased in June 2002, and lasting for 1 to 2 months, expired before he obtained internet access at Mimosa Lane on October 9, 2002. This claim, as demonstrated below, is, without question, false - he obtained internet access with AOL a year and a half before his first suspect-website subscription, in November 2000. He also contends that the other three subscriptions, to the Dark Feeling and Video-2000 websites, were made with a check card with the billing address of 1608 Harrodsburg Road. Thus, according to him, there is no connection to the Mimosa Lane premises in the Mimosa Lane Application and Affidavit. Based on his arguments regarding the April 5th Affidavit, Wagers would have the Court conduct a line by line scrutiny of the suspect affidavits. This is clearly contrary to the law in this Circuit. Rather, the Court must look at the "totality" of the circumstances surrounding the affidavit and search warrant. *Greene*, 250 F.3d at 479.

Wagers, however, does not explicitly address whether the April 8th Affidavit regarding the business at Harrodsburg Road sets forth sufficient facts supporting probable cause for the issuance of the affidavit. Even though he has not addressed this issue, the Court will, out of an abundance of caution, review this affidavit as well.

It is undisputed that the individual using the Spike20004u@aol.com email address between June 30, 2002, and June 3, 2003, reported two addresses: 1608 Harrodsburg Road (a billing address) *and* 3813 Mimosa Lane (a supplemental address). It is also clear that this account was registered to Wagers starting in November 2000. Further, the agents' independent investigation revealed that 3813 Mimosa Lane is Mr. Wagers primary residence according to public records databases. Additionally, Wagers established that AOL

account in November 2000, *nearly two yeas prior* to the first alleged wrongdoing. When he established his AOL account, Wagers also gave his night time phone number as 859-271-3484, which is listed for the residence at 3813 Mimosa Lane, and his day time number as 859-276-0594, his business phone. Furthermore, the Insight Communications billing address for Wagers' broadband account, which was activated on October 9, 2002, *prior* to the alleged use of two of the three websites, lists his billing address as 3813 Mimosa Lane. It is also undisputed that Wagers had the AOL account billed to the Harrodsburg Road address. He also listed both the Harrodsburg Road and Mimosa Lane locations on his Insight broadband connection. Every time Wagers subscribed to one of the three websites at issue, he used the foregoing AOL email account. Clearly, Wagers' connections to the internet were inextricably intertwined between the two addresses and the affidavits sufficiently set forth facts demonstrating this.

It is well-known that in today's "electronic" and "computer" age, many individuals, especially those engaged in professions mandating the use of computer technology, such as accountants, have computers both in an office and at home. It is also a well-known fact, and cannot honestly be disputed, that individuals often access their email and/or internet from both work and home. Here, the IP address in the customer transaction records from Video-2000 and Dark Feeling reflect that said IP address was assigned to Wagers during the same period in which he accessed the suspect websites. Unfortunately, web IP addresses do *not directly* reflect the geographic street address of the office, residence, or building from which an individual accesses his email and/or the internet. Instead, law enforcement officials must conduct research and rely upon the addresses and data provided by internet providers, such as AOL and Insight Communications, as well as billing addresses for those service

providers and/or credit card companies. Yet, the IP address assignment, namely to Wagers, is most telling in regards to which individual (Wagers) used it to access the sites containing the suspect material.

Additionally, the issue is not whether those websites have both "legal" and "illegal" pages to access, as Wagers contends in his brief;[1] the issue is whether there is "probable cause" to believe that evidence, fruits or instrumentalities of criminal activity may be found at the suspect premises. Mr. Wagers has a prior conviction relating to child pornography, which he does not dispute. He clearly had access to the internet from *many* locations, not just the Mimosa Lane and Harrodsburg Road locations, through his AOL account. Yet, his residence and business locations are certainly the most likely and suspect locations through which he would have accessed the internet. The question, then, is not whether he did or did not access child pornography through the suspect sites from those physical addresses, but, rather, giving the Magistrate Judge's decision great deference, whether there is a "fair probability" that evidence or fruits of criminal wrongdoing would be found. Clearly, the websites permitted

---

[1] In any event, Wagers' contention on this point is without merit. Specifically, although he argues that the alleged sites contain both "legal" and "illegal" content, the United States submitted screen shots from both the DarkFeeling and RedLagoon websites that contain exact and precise language indicating "all models are 14 and younger." [*See* DE # 37, Exs. A and B.] Thus, while those sites *may* contain "legal" material, which the United States concedes, two of the three websites at issue explicitly advertise and market that the materials, and specifically the pornography, contained on those sites are illegal in nature. This evidence lends further support in the finding of probable cause made by the Magistrate Judge.

access to child pornography. Mr. Wagers subscribed to the websites at various times and had internet access accounts from his home on Mimosa Lane and his business on Harrodsburg Road.

Furthermore, unlike the affiant in Gourde, the attesting officer undoubtedly averred that he believed child pornography could be found at the Defendant's residence and/or business. [Affidavits, ¶ 53] In child pornography cases, courts have repeatedly recognized that collectors of child pornography tend to retain their materials, and this Court agrees - it is probable that Mr. Wagers, having visited several websites known to have child pornography accessible on them, would have images, files, and/or electronic data evincing his downloading, possessing, viewing, accessing, or distributing child pornography. *See, e.g., United States v. Cox*, 190 F. Supp.2d 330, 333 (S.D.N.Y.2002). A host of district court decisions reflect rulings denying motions to suppress concerning child pornography searches several months *after* the alleged viewing or downloading of child pornography. *See United States v. Lamb*, 945 F. Supp. 441, 460 (N.D.N.Y.1996). *See also United States v. Ricciardelli*, 998 F.2d 8, 12 n. 4 (1st Cir.1993) (stating that "history teaches that collectors [of child pornography] prefer not to dispose of their dross, typically retaining obscene materials for years"); *United States v. Hay*, 231 F.3d 630, 633-36 (9th Cir.2000), *cert. denied*, 534 U.S.858, 122 S. Ct. 135, 151 L. Ed. 2d 88 (2001) (finding probable cause to believe child pornography would be found in defendant's computer *despite passage of six months* from single transmission of nineteen computer graphic files containing child pornography to defendant's computer). *United States v. Shields*, 2004 U.S. Dist. LEXIS 7090, 2004 WL 832937 (M.D.Pa. 2004).

Additionally, there is no need to make "inferences upon inferences" in this case, as the Court found in Gourde. Specifically, the only inference to be made herein is that the Defendant accessed child pornography on the websites at issue at some point. It is clear that he had internet access through either an AOL account or Insight's broadband connection; he had previously been convicted on child pornography charges; his internet connections were firmly attached through his home and/or business; he purchased several subscriptions at varying times to the websites at issue; and those websites, at various points in time, contained various child pornographic material. As a result, this case is clearly distinguishable from *Gourde*, because of the level of specificity contained in the affidavit supporting the search warrant.

Accordingly, it is reasonable to conclude and fairly probable that both the Mimosa Lane and Harrodsburg Road premises are reasonably connected to the viewing and/or accessing of the suspect websites. In other words, in the words of the Sixth Circuit, "the critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific things to be searched for and seized are located on the property to which entry is sought." *United States v. Rodriguez-Suazo*, 346 F.3d 637, 644 (6th Cir. 2003) (citations omitted). Based on the foregoing factors, the Magistrate Judge "had a substantial basis for finding that the affidavit established probable cause to believe that the evidence would be found at the place cited," both the Mimosa Lane residence and the Harrodsburg Road office. *See United States v. Davidson*, 936 F.2d 856, 859 (6th Cir.1991). The four corners of the affidavit, thus, support a finding of probable cause.

Thus, the Magistrate Judge made a simple, "practical, common sense decision [that] given all the circumstances set forth in the affidavit[s] before him . . . there [was] a fair probability that contraband or evidence of a crime will be found" at both the Mimosa Lane residence and the Harrodsburg Road office. *See Illinois v. Gates*, 462 U.S. at 238. Wagers indisputably subscribed to at least three (3) websites containing illegal child pornography and this, in combination with the other factors set forth in the affidavits and discussed herein, unquestionably satisfies the probable cause requirement. *See United States v. Bailey*, 272 F. Supp. 2d 822, 824-25 (D.Neb. 2003) (holding that "knowingly becoming a computer subscriber to a specialized internet site that frequently, obviously, unquestionably and sometimes automatically distributes electronic images of child pornography to other computer subscribers alone establishes probable cause for a search of the target subscriber's computer even though it is conceivable that the person subscribing to the child pornography site did so for innocent purposes and even though there is no direct evidence that the target subscriber actually received child pornography on his or her computer."). Giving Magistrate Judge Todd the great deference required by the Supreme Court, probable cause existed for the issuance of the search warrants at issue on the two Lexington premises. *See United States v. Payne*, 341 F.3d 393 (5th Cir. 2003.) ("While the generalization alone might be insufficient to render official reliance reasonable, other facts in the affidavit taken together with generalizations founded upon training and experience could support reasonable reliance. Other facts in the affidavit lend support to the inference that evidence of child sexual exploitation might be discovered in Payne's home. We conclude, considering the affidavit and the circumstances surrounding issuance of the warrant, that the good faith exception applies"). *United States v. Froman*, 355 F.3d 882, 891 (5th

Cir.2004) (holding that it is common sense that a person who voluntarily joins a website containing child pornography, even one who maintains a membership for as little as one month, would download such pornography from the website and have it in his possession).

In any event, even if probable cause was not established from the four corners of the affidavits, the "good faith" exception set forth in *United States v. Leon*, 468 U.S. 897, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984), would be applicable herein and render the searches valid. In a case discussing this exact issue, *United States v. Rice*, 358 F.3d 1268 (10th Cir.2004), the defendant appealed the denial of his motion to suppress. He argued that the affidavit did not specify how the sexually suggestive websites listed in the affidavit were linked to emails and that it did not indicate that he actually ever visited those websites or obtained or possessed anything which was in fact child pornography. *Id.* at 1274. The district court held that the affidavit provided the magistrate judge with sufficient information from which he could reasonably conclude there was probable cause to believe that evidence of child pornography would be found at the defendant's residence. *Id.* The trial court also held that, even if the affidavit failed to establish probable cause, suppression was unnecessary because the agents executing the warrant acted in objectively reasonable, good-faith reliance on the warrant. *Id.* The affidavit in question, similar to the ones at issue in this case, stated that several sexually explicit emails had been received by an individual with a certain AOL email account, riceone2000@aol.com, and that said user name belonged to the defendant. *Id.* The emails also clearly provided access to websites providing child pornography, like the websites at issue herein did. Even though the affidavit did not state that the defendant accessed those pages containing the child pornography, the Court ultimately affirmed the trial

court under the good faith exception set forth in *United States v. Leon*, 468 U.S. 897, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984). *Rice*, at 1274. These facts seem very analogous to the instant action and this "good faith" exception would remedy any failings in the April 5th or April 8th Affidavits.

C. AOL Affidavit

Finally, concerning the AOL Affidavit, Wagers contends that the AOL affidavit does not connect the premises to be searched with the crimes to be investigated. He avers that this affidavit does not reference his usage of email and that it is fatally deficient in connecting the alleged wrongful activity with the items to be searched. He also complains that there is insufficient nexus between the place to be searched and the evidence sought.

Contrary to Wagers' assertion, he used his AOL screen name and account to establish accounts with at least three (3) suspect websites containing child pornography. This account was also used to access two (2) additional websites. The April searches at his residence and business resulted in the seizure of files evincing that Wagers had used AOL instant messenger to receive, share, and/or download child pornography files. The affidavit sought information pertaining to AOL's business records, including log files, electronic images, screen names and account information, *not only email records,* that would reflect evidence of criminal activity related to the foregoing facts.

Because Wagers had an account with AOL for 3 years, and had used his screen name and account in the manner previously discussed, as well as the fact that AOL provides email, file and messenger services through which an individual can access the internet and share files, the AOL

affidavit seems sufficient to establish probable cause for the search of those premises and the data sought. *See United States v. Sassani*, 139 F.3d 895 (Table), 1998 WL 89875 at *6 (4th Cir. 1998) (unpublished) (recognizing that a review of relevant federal cases makes clear that courts routinely find search warrants allowing seizure of a computer and all its associated printing, storage, and viewing devices constitutional in child pornography cases because these items "not only may contain evidence of distribution of child pornography, but are also the instrumentalities of the crime.") Accordingly, the Court finds Wagers' arguments concerning the AOL Affidavit unconvincing as well.

IV. MOTION FOR LEAVE

Concurrent with his Reply to the Motion to Suppress, Wagers filed a Motion for Leave to place evidence in the record absent a stipulation. [DE # 36] However, this request was merely included in the styling of his reply brief and he devotes a mere sentence to it in his brief. Specifically, he asks that if the United States contests that the websites contained legal and illegal material, he should be able to put evidence in the record indicating that the websites contained both legal and illegal material at the time be viewed those sites. However, Wagers does not cite any authority or otherwise explain what this evidence would be or consist of. In any event, for the reasons stated in footnote 1, *supra,* this request would be without merit. Thus, Court will deny this motion as well. *See also* LCrR 12.1.

V. CONCLUSION

Based on the foregoing facts and case law, the Court finds that the Defendant has not sustained his burden of proof as required by *United States v. Feldman*. Reviewing the

evidence in the light most favorable to the government, *United States v. Garza*, the affidavits sufficiently show probable cause on their face and the motion will be denied. Further, the affidavits being sufficient on their face, there is no need for an evidentiary hearing in this case.

Accordingly, for the reasons enumerated in this Memorandum Opinion, and the Court being otherwise sufficiently advised, it is hereby ORDERED that:

(1) No evidentiary hearing is necessary in this matter;

(2) The Defendant's Motion To Suppress [DE # 30] is DENIED; and

(3) The Defendant's Motion for Leave to place evidence in the record absent a stipulation [DE # 36] is DENIED.

This 12th day of October, 2004.

APPENDIX D

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
LEXINGTON

Case No. 04-5051M

[Filed April 5, 2004]

IN THE MATTER OF THE	)
SEARCH OF:	)
The Residence at	)
3813 Mimosa Lane	)
Lexington, Kentucky 40517	)
	)

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

I Sean Lichner being duly sworn depose and say:

I am a(n) Special Agent with the Department of Homeland Security, U.S. Immigration and Customs Enforcement and have reason to believe that __ on the person of or X on the property or premises known as the residence at 3813 Mimosa Lane, Lexington, Kentucky 40517, which is two-story sided building, green in color, with an attached two-car garage. The front of the building has three windows, a doorway and the attached two-car-garage facing Mimosa Lane. The

residence is described in Attachment A which is attached hereto and made a part hereof.

in the EASTERN District of KENTUCKY there is now concealed a certain person or property, namely a computer, computer hardware, and those items more specifically described in attachment "B'" which is attached hereto and made a part hereof.

which is evidence of a crime, contraband, fruits of crime, other items illegally possessed, or property designed for use, intended for use, or used in committing a crime, concerning a violation of Title 18 United States Code, Section(s) 2252(b)(l), 2252(a)(2) & 2252(a)(4)(B).

The facts to support a finding of Probable Cause are as follows:

SEE Attached Affidavit of Special Agent Scan Lichner which is attached hereto and made a part hereof.

Continued on the attached sheet and made a part hereof.
✓ Yes ___ No

/s/
Signature of Affiant

Sworn to before me, and subscribed in my presence

April 5, 2004
Date

at Lexington, Kentucky
City and State

James B. Todd, U.S. Magistrate Judge
Name and Title of Judicial Officer

/s/
Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH

I, Sean Lichner, being duly sworn, depose and state:

1. I am a Special Agent with the Department of Homeland Security, United States Immigration and Customs Enforcement (ICE), assigned to the Resident Agent In Charge Northern Kentucky. I have been so employed since April 7, 2003. As part of my daily duties as an ICE agent, I am responsible for investigations involving the importation and distribution of child-pornography and criminal violations relating to the sexual exploitation of children. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 United States Code ["U.S.C."] § 2256).

2. This Affidavit is made in support of Application for Search Warrant for the following location:

   (A) A residential dwelling located at 3813 Mimosa Lane, Lexington, Kentucky 40517 (the "SUBJECT PREMISES"). The SUBJECT PREMISES to be searched is more particularly described as a two-story sided building, green in color, with an attached two-car garage. The front of the building has three windows, a doorway and the attached two-car garage facing Mimosa Lane.

   (B) Lyman Wagers also has a business known as Wagers Tax Firm, Inc., located at 1608 Harrodsburg Road, Lexington, Kentucky 40504 (the "SUBJECT BUSINESS"). Your affiant has mentioned the

SUBJECT PREMISES in this affidavit in the event it becomes necessary to apply for a search warrant for the business location. If it becomes necessary to apply for a search warrant for the business, your affiant will rely on the information set forth in this affidavit. The business is more particularly described as a two-story red-brick building with eight windows and the front door facing Harrodsburg Road. There is a sign outside the business labeled "Wagers Tax Firm, Inc."

3. The purpose of this application is to seize evidence of violation of Title 18, United States Code, Sections, 2252 (b)(l); 2252 (a)(2) and 2252 (a)(4)(B), for a conspiracy to receive, attempt to receive, the receipt and the possession of child pornography, respectively. Based on the facts set forth in this affidavit, I have reason to believe that evidence of the previously listed criminal violations will be found at the location listed in paragraph 2(A).

4. Title 18, United States Code, Section 2256, defines the term child pornography as meaning "means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where

(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

(B) such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct;

(C) such visual depiction has been created, adapted, modified to appear that an identifiable minor is engaging in sexually explicit conduct; or

(D) such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

5. Title 18, U.S.C., Section 2256(2) defines sexually explicit conduct as meaning "actual or simulated

(A) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

(B) bestiality;

(C) masturbation;

(D) sadistic or masochistic abuse; or

(E) lascivious exhibition of the genitals or pubic area of any person;"

6. I am familiar with the information contained in this Affidavit based upon the investigation I have conducted, the investigation of other law enforcement officers and conversations with other law enforcement officers who have engaged in numerous investigations involving child pornography.

7. As a result of the investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, as set for the above will be located at the SUBJECT PREMISES.

8. The investigation has revealed that an individual employing the e-mail account Spike20004u@aol.com, subsequently identified as Lyman E. WAGERS, Jr., purchased at least four (4) subscriptions to websites that were distributing child pornography, and that there is probable cause to believe that Spike20004u@aol.com subscribed to these websites using computers that are located at the SUBJECT PREMISES and at the SUBJECT BUSINESS.

9. The information set forth below is provided as a broad overview of the investigation conducted to date. It does not include a listing of all investigative techniques employed or even the full and complete results of any of the listed investigative efforts.

Overview of the Underlying New Jersey Investigation

10. The United States Attorney's Office for the District of New Jersey ("USAO DNJ"), the U.S. Department of Justice's Child Exploitation and Obscenity Section ("CEOS"), and the New Jersey offices of ICE, Internal Revenue Service, Criminal Investigations Division ("IRS CID"), the United States Postal Inspection Service ("USPIS"), and the Federal Bureau of Investigation ("FBI") conducted a joint investigation (the "New Jersey Investigation") of Regpay, a third-party billing and credit card aggregating company. The investigation revealed that Regpay conspired with other website operators to commercially distribute child pornography by providing the other websites with billing and credit card aggregating services, and taking a percentage of the other websites' illegal proceeds. The investigation also revealed that Regpay itself operated several websites that sold child pornography.

Regpay's Billing Service Operations for Child Pornography Websites

11. The New Jersey Investigation revealed that (1) Regpay operated regpay.com, a website that it used to conduct its billing services; (2) the regpay.com website was housed on a server at Verio, Inc.; (3) Regpay leased IP addresses at Rackspace Managed Hosting ("Rackspace"), and Regpay housed its customer databases including customer transaction records on servers at Rackspace; (4) Regpay obtained the assistance of Connections USA, Inc. ("Connections"), a Florida Domestic Corporation located in Florida, to coordinate its billing and credit card processing services; and (5) Connections processed at least $3,000,000 for Regpay between November 1, 2002 and April 30, 2003 including credit card transactions that Connections processed for Regpay through Iserve.com ("Iserve")[1], an e-commerce company that purportedly provides a variety of payment processing services, including the performance of credit card and check processing, for computer websites that offer membership subscriptions to the public. During the course of the New Jersey Investigation of Regpay, federal agents, acting in an undercover capacity ("the UC Agents") became paid subscribers/members of websites that used Regpay as a billing company.[2] In many instances, when a UC agent subscribed to a website or purchased a membership to a website using a credit card, a billing page automatically

---

[1] Iserve.com is a fictitious business name owned by Connections.

[2] The investigation revealed that not all of those websites used Regpay exclusively; some of those websites used multiple billing companies.

appeared on the computer screen, which sought personal and financial information, and revealed that the transaction was being processed by or through Regpay. At the top of the billing page was a logo containing the letters "rp" and the word "regpay," as well as the name of the website to which the undercover agent was seeking to subscribe or purchase. After completing the form, which included providing a credit card number to be used for the purchase, each UC agent was instructed to "hit the JOIN NOW! button" on the screen. Shortly after clicking on the "JOIN NOW!" button, each UC agent received a message from Regpay stating that Regpay successfully charged the provided credit card. The message provided each agent with a transaction number, log-in information, and a password to log into the members-only site. The message stated that "Iserve will appear on your credit card statement as a beneficiary of this transaction." In some instances, shortly after receiving the above described message from Regpay, the agent/purchaser also received a message from "Iserve.com," thanking the customer for using Regpay, and indicating that Iserve would appear on the customer's billing statement. The message thereafter provided the date and time of the transaction, a transaction number, and the amount of the transaction. Records later obtained from the banks that issued the credit cards used in several of the undercover purchases listed "Iserve" for each of these transactions.

12. As part the New Jersey Investigation of Regpay, information housed on various servers that helped facilitate customer transactions for hundreds of websites was seized from several locations in the United States pursuant to several search warrants. After analyzing the customer data, the ICE forensic agents identified tens of thousands of purchases of child pornography between

January 2003 and July 2003 associated with those websites, that is tens of thousands of confirmed subscriptions which granted purchasers access to those websites.

13. Further, undercover purchases made by ICE agents (described above in paragraph 11) prior to executing search warrants for Regpay's customer transactional information, were found to be recorded in the database found on Regpay's Rackspace server. ICE forensic specialists determined that the Regpay database operated under a database management system called "MySQL," and that this database's contents and structure were thus legible. In other words, upon finding that the database operated using the MySQL system, and that the coding was intelligible, ICE forensic experts determined that they could decipher Regpay's customer transactional data and use it to identify the subscribers/members of the websites to whom Regpay had provided third-party billing services.

14. At various times between February and September 2003, federal agents verified that at least 21 websites that Regpay had been servicing were still active, accessible on the Internet, and contained child pornography. They did so by accessing these websites on the Internet and subscribing to those sites that advertised child pornography or showed actionable images in their "preview" or "nonmember" sections. Although the federal agents have no way of ascertaining the actual contents of each website on the various dates customers would have visited the websites, the federal agents were able to verify that on those dates the websites were visited by the federal agents, the websites contained child pornography as defined by federal law.

15. Based on the customer transaction records obtained through the execution of search warrants which revealed customer subscriptions to websites that federal agents had independently verified as containing child pornography, the ICE Cyber Crimes Center identified various individuals as subscribers to websites containing child pornography. In turn, the ICE Cyber Crimes Center sent leads to field offices across the country. The search warrant of the SUBJECT PREMISES and SUBJECT BUSINESS evolved from one of those leads.

ICE Analysis of Regpay's Customer Transactional Data

16. By way of background, and as noted earlier, Regpay's customer transactional information was found to be recorded in the database found on Regpay's Rackspace server, which was searched pursuant to a warrant. ICE forensic specialists examined the source code[3] or 'scripts' used to populate the various fields in the Rackspace database, and determined how each of the fields pertaining to the websites' customers (hereinafter, "subscriber(s)/member(s)") were generated by Regpay's web page programming.

17. The ICE forensic specialists learned that when Regpay had served as the billing company for the members-only websites that contained child pornography, the subscribers/members of these websites would input certain information when a billing page would appear. That information was then recorded by Regpay in fields that it maintained in its database.

---

[3] Source code is computer software programming statements and instructions.

18. The fields that appeared in the Regpay customer information data, which ICE forensic specialists determined had been completed based upon information provided by the websites' subscribers/members were:

    1. fname, referring to the website subscriber/member's first name as entered on the Regpay form;

    2. lname, referring to the website subscriber/member's last name of the customer as entered on the Regpay form;

    3. addr, referring to the website street address as entered on the Regpay form;

    4. city, referring to the website subscriber/member's city as entered on the Regpay form;

    5. state, referring to the website subscriber/member's state as entered on the Regpay form;

    6. zip, referring to the website subscriber/member's zip code as entered on the Regpay form;

    7. phone, referring to the website subscriber/member's telephone number as entered on the Regpay form;

    8. country; referring to the website subscriber/member's country as entered on the Regpay form;

    9. ccnumber, referring to the website subscriber/ member's credit card number as entered on the Regpay form;

10. cvv2, referring to the website subscriber/member's three digit number from the credit card, as entered on the Regpay form;

11. card_type, referring to the website subscriber/ member's credit card, as entered on the Regpay form;

12. expmonth, referring to the website subscriber/ member's credit card, as entered on the Regpay form;

13. expyear, referring to the website subscriber/member's credit card expiration date, as entered on the Regpay form; and

14. email, referring to the website subscriber/member's e-mail address as entered on the Regpay form.

19. Federal agents who had subscribed, in their undercover capacity, to one or more websites containing child pornography, and whose transactional information was found to be among the consumer transaction data seized during the searches of Rackspace's Regpay servers, verified that the information pertaining to the transactions they had conducted was contained as each of them had input it in the Regpay database.

20. ICE Cyber Crime Center determined that a field in the "members" table of the Regpay database called "siteid" was a unique identifier that correlated each subscription purchase to a website listed in the "sites" table of the database. ICE agents were able to determine which website each customer purchased by correlating the siteid entry in the "members" table to the relevant "sites" table entry.

21. In addition to determining which fields were completed by subscribers/members, forensic specialists at ICE's Cyber Crime Center also determined that the following fields on the Regpay customer transaction forms were generated automatically by Regpay's coding or script, and then stored in Regpay's MySQL database:

    (a) login, referring to the access user name;

    (b) passwd, referring to a randomly generated 8 character password; and

    (c) regtime; referring to the hour:minute:second the script ran (according to the host machine).

22. The fact that the fields referenced in paragraph 21 were computer-generated and were relayed to subscribers/members prior to their entry into the purchased websites is significant. Based on my own experience and conversations with other agents, although a website subscriber/member could easily provide a false name when subscribing to websites, the subscriber/member most certainly had to provide a legitimate credit card number and an e-mail account in order to subscribe to/become a member of the website. This is because the subscriber/member would have been required to provide a valid e-mail account in order to actually enter the website in which he or she was interested in. In fact, entry into the members-only websites that contained child pornography would most likely have been preceded by the subscriber/member's receipt of an e-mail that, along with confirmation that the credit card purchase had been successfully completed, included the subscriber/member's computer-generated password, as well as instructions needed to access the

website (see paragraph 11). Inaccurate credit card or e-mail information would most likely have precluded entry into the website. Given the likely accuracy of the e-mail address and credit card information provided by the subscriber/member, federal agents focused on that information to identify subscribers/members.

Probable Cause to Search the Subject Premises

23. Upon receipt of a lead from the ICE Cyber Crimes Center, the undersigned affiant, working with other agents in the Ft. Mitchell Field Office, the United States Postal Inspection Service and the Kentucky State Police commenced an investigation, which revealed that between June 30, 2002 and June 3, 2003, an individual whose e-mail address is Spike20004u@aol.com, with reported addresses of 1608 Harrodsburg Road, Lexington, Kentucky 40504, and 3813 Mimosa Lane, Lexington, Kentucky 40517 who used credit card numbers are 3712 7076 9432 006 and 4427 4203 4012 6520, subsequently identified as Lyman E. WAGERS, JR, paid to subscribe to four (4) websites later confirmed to contain child pornography. Based on the investigation and my training and experience, there is probable cause to believe that WAGERS is a recipient and collector of child pornography, and that evidence of his conspiracy to receive, attempt to receive, the receipt and the possession of child pornography will be found at his residence, the SUBJECT PREMISES.

24. More specifically, in the course of analyzing the Regpay customer transactional data that had been seized pursuant to the search warrants referenced above, it was discovered that one of the individuals who was a subscriber to the following members-only websites: http://redlagoon.com,

http://www.video2000.com/ and http://www.darkfeeling.com, used and e-mail account of Spike20004u@aol.com. The investigation further revealed that the individual using the e-mail account/user name[4] Spike20004u@aol.com, provided addresses of 1608 Harrodsburg Road, Lexington, Kentucky 40504 and 3813 Mimosa Lane, Lexington, Kentucky 40517 and the telephone number 859-271-3483. This individual used a series of credit cards to purchase access to members-only websites between June 30, 2002 and June 3, 2003, including, but not limited to, a card issued by American Express Travel Services ("American Express") and a card issued by Bank One NA ("Bank One").

25. The customer transaction records indicate that four of the members-only sites' purchased by Spike20004u@aol.com permitted electronic access to child pornography. Specifically, Spike20004u@aol.com purchased access to the following members-only sites on or about the following dates:

    1. http://redlagoon.com - June 30, 2002;

---

[4] An e-mail account/user name/screen name is the name a person uses to identify himself or herself when logging onto a computer system or online service. Both a username (user ID) and a password are required. Typically, with an Internet e-mail address, the user name is the address that precedes the @ sign. For example, harryW is the username in harryW@usdoj.gov. ISPs call the username a "screen name." For purposes of the instant affidavit, the undersigned Affiant has used the terms "user name" (or, in the case of AOL, "screen name"), and "e-mail account" interchangeably.

2. http://www.Video-2000 - March 22, 2003;

3. http://www.dark-feeling.com - April 15, 2003; and

4. http://www.Video-2000 - June 3, 2003.

26. From on or about February 26, 2003 though on or about August 02, 2003, federal agents made the following undercover purchases of memberships to websites containing child pornography:

(i) **www.redlagoon.com/lustgallery aka www.lust-gallery.com:** On March 26, 2003, a federal agent, while acting in an undercover capacity, purchased a one-month membership, in the approximate amount of $49.95 + additional fees, to a website entitled "Lust Gallery". A credit card number was provided to effect this transaction. The information appearing in the address box of my internet browser, while viewing the subscription page was http://64.239.16.69/sale.cgi?s=91111&ad=ad00094313. The name "regpay" appeared in relatively large letters on the webpages as the main billing company and on the approval page in smaller type was the name "ISERVE", which was listed as the "beneficiary of this transaction".

Additional information on the approval page included the transaction number: 178628, a login: me01793961, a password: 4YHdhagp, and a members UBL of http://69.0.255.118/members/. Using this information, the undercover agent accessed the website and downloaded images of children engaged in sexually explicit conduct.

Contained on the website were numerous pictures depicting minor females in various poses and states of undress. Specifically, three of the images contained on the website are described as follows:

1. 35&back=30: This image features a pubescent, nude female raising the left leg of a second prepubescent, nude female, exhibiting the genitals of the second prepubescent female.

2. 7&back=0: This image features a closeup of the genital and anal area of a pubescent nude female with her legs apart exhibiting her genitals.

3. 31&back=30: This image features a closeup of the genital area of a pubescent nude female squatting on the floor with her legs spread apart.

(ii) On August 1, 2003, a federal agent, while acting in an undercover capacity, purchased a 31 day membership to a website entitled "Video-2000" aka www.video-2000.com, site URL name http://www.video-2000.net/members/index/html using master card gift card number 553772001581390 for approximately $50.90. The membership was purchased with a credit card provided to a billing company identifying itself as Cardspay. Cardspay thereafter provided the agent with a login number, password, and the member URL site with the web address: http://www.video-2000.net/members/index/html. Using this information, the agent accessed the website and downloaded videos of children engaged in sexually explicit conduct.

(iii)**http://www.darkfeeling.com:** On July 21, 2003, a federal agent, acting in an undercover capacity, purchased

a one-month membership, for approximately $57.90, to a website with a URL of www.darkfeeling.com. The undercover agent used a MasterCard credit card. This credit card information was provided to a billing company identifying itself as "Regpay". Regpay thereafter provided the agent with a transaction number: 295276, a login: me01901415, a password: sTh8mbXM, and members URL of http://69.0.237.222/members. Using this information, the undercover agent accessed the website and downloaded images of children engaged in sexually explicit conduct. The home page of the website features images of several females of various ages in multiple poses, and an invitational to become a member of the website. Contained within the website were numerous pictures of young girls in various poses and states of undress. Specifically, three of the images contained in this website are described as follows:

1. DSCN8577.jpg in Set #79: This image features a nude prepubescent female sitting in a chair. Her right leg is bent at the knee and her leg is leaning slightly outward, her left leg is bent at the knee and is lying out to the side, parallel to the floor. Her legs are parted in approximately a ninety degree angle, her genital area is exposed as well as her undeveloped breasts. Her left hand is grasping her left shin. The photo was taken from a frontal viewpoint.

2. P1010370 Set #67: This image features a nude prepubescent female lying on a bed on her back with her legs spread apart, exposing her genital area. Her left-leg is bent at the knee and is leaning out to the side, her right leg is outstretched, lying flat against the bed.

3. DSCN2327.jpg Set #60: This image features a nude prepubescent female sitting on what appears to be a shag carpet on the floor. The nude prepubescent female is leaning back against an item of furniture with her legs spread apart, exposing her genital area. Both of her legs are bent up at the knees and are parted, leaning out away from her body. Her hands are grasping her ankles.

27. The undersigned Affiant reviewed several DVD disks sent to the Ft. Mitchell ICE field office, which contained digitally preserved copies of the above-listed websites purchased by undercover agents. The undersigned Affiant has also personally reviewed the content of the above websites purchased by Spike20004u@aol.com, that were digitally preserved and the content copied to the hard drive by ICE Agents at the Cyber Crimes Center in Fairfax, Virginia. An agent with expertise in the field of child pornography reviewed several images from each of those websites and concluded that they constitute child pornography.

28. America Online, Inc. ("AOL") is an ISP through which the user name Spike20004u@aol.com was issued. A Subpoena was sent to AOL following the receipt of the lead from the Cyber Crimes Center. Records returned from AOL as a result of the Subpoena indicate that the e-mail address Spike20004u@aol.com is associated with Lyman WAGERS whose billing address is 1608 Harrodsburg Road, Lexington, Kentucky 40504, the SUBJECT BUSINESS.

29. AOL also confirmed that WAGER'S account was activated on November 24, 2000; that the account was

active at the time that each of the purchases described above were made; and that WAGERS gave a night phone number of 859-271-3483 and a day phone number of 859-276-0594.

30. AOL also provided the following screen names/e-mail accounts that belong to WAGERS: cruelsadistm, k9trainer4yf, leewagers2001 and slavemasterlee.

31. The AOL billing records indicate that the method of payment for AOL services for WAGERS use of AOL is by a Visa credit card. The number listed on the AOL billing records is 4427 4203 4012 6520. This Visa card number is identical to WAGER'S Bank One card number that was listed in the Rackspace customer records.

32. On or about June 30, 2002, WAGERS purchased access to http://redlagoon.com. The customer transaction records from Rackspace indicate lis[illegible]he IP address of the computer that was accessing http://redlagoon.com as 172.150.168.17. A trace of the IP address using the website ARIN WHOIS reveals that the IP address is owned by AOL.

33. Insight Communications ("Insight") is an ISP that is utilized by WAGERS. Records returned from Insight following the issuance of a Subpoena reveal that WAGERS utilizes high speed internet access at the SUBJECT PREMISES and also has video programming. The billing addresses listed on the WAGER'S Insight records are 3813 Mimosa Lane, Lexington, Kentucky, the SUBJECT PREMISES and 1608 Harrodsburg Road, Apt. A, Lexington, Kentucky, the SUBJECT BUSINESS. Additionally, Insight provides several telephone numbers, including 859-27 1-3483 as the number listed to 3813

Mimosa Lane, Lexington, Kentucky, the SUBJECT PREMISES and 859-276-0594 as the number listed to 1608 Harrodsburg Road, Apt. A, Lexington, Kentucky, the SUBJECT BUSINESS.

34. Insight also confirmed that WAGER'S account was activated on October 9, 2002 and that the account was active at the time that each of the purchases described above were made.

35. On March 22, 2003 a purchase was made for access to http://www.video2000.com. The IP address that a computer used to access the Internet to purchase a membership was listed on the customer transaction records as 12.222.198.103. On April 15, 2003, a purchase was made for access to http://www.darkfeeling.com. The IP address of the computer that accessed the Internet to purchase a membership to http://www.darkfeeling.com was listed on the customer transaction records as 12.222.198.103. On June 6, 2003, a purchase was made for access to http://www.video2000.com. The IP address of the computer that accessed the Internet to purchase a membership was listed on the customer transaction records as 12.222.198.103. The information Insight provided to Agents/Officers as a result of a Grand Jury Subpoena reveals that the IP address 12.222.198.103 was assigned to Lyman E. WAGERS JR. during the time period from March 6, 2003 to June 3, 2003.

36. Following receipt of the lead from Newark, it was determined that the purchase made for access to http://redlagoon.com on June 30, 2002 was made with WAGER'S card number 3712 7076 9432 006. The purchase price, according to the Rackspace records, was

$67.90. The card number was identified as being issued by American Express. A Subpoena was sent to American Express for financial and ownership records for card number 3712 7076 9432 006. The records returned from America Express list the card owner as Lyman E. WAGERS JR. with an address of 1608 Harrodsburg Rd., Lexington, Kentucky 40504-3706. The American Express account for WAGERS was activated on December 13, 1996 and is currently an active account. The financial records returned from American Express list two charges to "ISERVE FT. LAUDERDALE FL" on June 27, 2002. Both charges were in the amount $67.90. Furthermore, according to American Express, card number 3712 7076 9432 006 was not reported lost or stolen during the period of the purchases.

37. Pursuant to the receipt of the information from the Cyber Crimes Center, it was determined that the purchase made for access to (i) http://www.video2000.com on March 22, 2003; (ii) http://www.darkfeeling.com on April 15, 2003; and (iii) http://www.video2000.com on June 3, 2003 were made with card number 4427 4203 4012 6520. This card number was identified as being a checking card issued by Bank One. A Subpoena was sent to Bank One for financial and ownership records on card number 4427 4203 4012 6520. The records returned from Bank One list Wagers Tax Firm Inc. as the primary account holder for card number 4427 4203 4012 6520 with a billing address of 1608 Harrodsburg Road, Lexington, Kentucky 40504. The account number is listed as 615074150 and the type of account is listed as a Bank One business checking account. WAGERS signed the business signature card as President of Wagers Tax Firm Inc. The card was activated on January 3, 2003 and is currently active. Furthermore, the Bank One Subpoena Compliance

Department has indicated that there were no disputes reported during the time period that included the three purchases referenced above.

38. The Bank One financial records list a charge to "Iserve *8009290300" on March 21, 2003 in the amount of $67.90. This charge corresponds to the March 22, 2003 listing found in the Rackspace records for access to http://www.video2000.com. The Rackspace records list the amount paid as $67.90.

39. The financial records from Bank One list a charge for "Iserve *8009290300" in the amount of $82.90 on April 14, 2003. This is within a day of the listing in the Rackspace records for a purchase made by WAGERS for in the amount of $82.90 for access to http://www.darkfeeling.com. The amount listed in the Rackspace records for the WAGERS'S purchase of access to http://www.darkfeeling.com is also listed as $82.90.

40. The financial records from Bank One list a charge on June 2, 2003 for Iserve *8009290300. The financial records list the charge as $67.90. The records found with Rackspace list a purchase made by WAGERS on June 3, 2003 for access to http://www.video2000.com. The Rackspace records list the amount paid for access to http://www.video2000.com as $67.90.

41. A further review of the Bank One financial records show that in addition to the charges for Iserve referenced above, charges for ISERVE appear eight (8) additional times between February 6, 2003 and June 21, 2003. The fact that Iserve appears eight (8) additional times on WAGER'S Bank One financial records is relevant to the underlying investigation. Your affiant has learned through

discussions with other agents and officers and that over a over majority of Iserve's business consisted of third party billing for web sites that allowed access to child pornography for a fee.

42. A study of the monthly billing records for Bank One shows that the card has over twenty-five (25) charges from third party billing services. Specifically, at least fifteen (15) charges relate to Rigva, Latvia and St. Petersburg, Russia. Based on your affiant's experience with the New Jersey investigation and discussions with other agents and officers, it is known that countries in the former Eastern block region, including Latvia and Russia, are source countries for child pornography that appears on the Internet.

43. Additional information obtained from public databases reveals that WAGERS lives at 3813 Mimosa Lane, Lexington, Kentucky 40517 and has a home phone number of 859-271-3483 and business phone number of 859-276-0594.

44. A Commonwealth of Kentucky, Department of Motor Vehicles check revealed that Lyman E. WAGERS, JR., Date of Birth, 12/23/1948, possesses a Commonwealth of Kentucky Drivers License. The check listed the WAGER'S address as 3813 Mimosa Lane, Lexington, Kentucky. Two vehicles are listed as registered to businesses affiliated with WAGERS and/or WAGERS. The first, which is registered to Lyman Wagers PSC/Lyman Wagers, is a 2004 Lexus, green in Color, bearing Kentucky license plate number 2419JR, vehicle identification number JTJBT20X730004413. The second, which is registered to Wagers Tax Firm Inc./Lee Wager, is a 2000 Lexus, gold in color, bearing Kentucky license

plate number 582FMA, vehicle identification number JT6HF10U5Y0113410.

45. A query of the Commonwealth of Kentucky online business database lists Lyman E. Wagers as the Incorporator, Registered Agent, and sole Officer of a Kentucky corporation known as Wagers Tax Firm, Inc. The address listed is 1608 Harrodsburg Road, Lexington, Kentucky 40504, the SUBJECT BUSINESS. The standing of the business is listed as being in good standing and the status is listed as active.

46. On October 31, 1997, Lyman Wagers entered a plea of guilty to a one count criminal Information charging him with a violation of Title 18, United States Code, Section 2252(a)(4)(B), for the possession of child pornography. Pursuant to Kentucky Supreme Court rules, Wagers was automatically suspended from the practice of law following his guilty plea. On December 18, 1997, the Kentucky Supreme Court entered an order automatically suspending Wagers from the practice of law effective November 1, 1997, pending further orders of the court. There is no indication that Wagers has resumed the practice of law. Notwithstanding Wagers' suspension from the practice of law, search team members will be briefed on the possibility that stored confidential files could be stored at either the business or residence. If such files are located, the files will immediately be isolated and looked at by a separate search team to ensure that no confidential information is compromised. Any search of such records would be for the sole and limited purpose of determining if sexually explicit images were secreted with the any archived client files. Also, as a result of his conviction, Wagers is listed as a sex offender on the Commonwealth of Kentucky State Police Registry

online database. WAGERS is listed as Lyman E. WAGERS, Jr., with a registration date of March 3, 1999. The registry lists WAGER'S address as 3813 Mimosa LN, Lexington, Kentucky 40517 as of December 1, 2003.

47. A Postal Inspector verified through the United States Postal Service database that WAGERS receives mail at 3813 Mimosa Lane, Lexington, Kentucky 40517 that is, the SUBJECT PREMISES and at 1608 Harrodsburg Road, Lexington, Kentucky 40504 the SUBJECT BUSINESS. Additionally, a postal carrier confirmed on January 17, 2004 that WAGERS has continued to accept mail at the SUBJECT PREMISES and that no other person is listed as a mail recipient at the SUBJECT PREMISES.

48. Surveillance of the SUBJECT PREMISES revealed that on March 1, 2004 and on March 12, 2004 a Lexus with license plate number 2419JR was parked behind the business during business hours.

49. Based upon the information provided by AOL, Insight, Bank One, American Express, The United States Postal Service, the Commonwealth of Kentucky State Police Sex Offender Registry, and the Kentucky Secretary of State, there is probable cause to believe that the individual using the user or screen name Spike20004u@aol.com is Lyman E. WAGERS JR., who lives at the SUBJECT PREMISES and works at the SUBJECT BUSINESS.

50. Based on the foregoing there is probable cause to believe that records, documents and materials relating to WAGER'S receipt and possession of child pornography are located in WAGER's residence, the SUBJECT PREMISES.

Specifics Regarding the Seizure and Searching of Computer Systems

51. Based on my own experience and consultation with other agents who have been involved in the search of computers and retrieval of data from computer systems and related peripherals, and computer media, there are several reasons why a complete search and seizure of information from computers often requires seizure of all electronic storage devices, as well as all related peripherals, to permit a thorough search later by qualified computer experts in a laboratory or other controlled environment:

    1. Computer storage devices, such as hard disks, diskettes, tapes, laser disks, and Bernoulli drives, can store the equivalent of hundreds of thousands of pages of information. Additionally, when an individual seeks to conceal information that may constitute criminal evidence, that individual may store the information in random order with deceptive file names. As a result, it may be necessary for law enforcement authorities performing a search to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This review and sorting process can take weeks or months, depending on the volume of data stored, and would be impossible to attempt during a search on site; and

    2. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even those who are computer experts to specialize in some systems and applications. It is difficult to know

before a search what type of hardware and software are present and therefore which experts will be required to analyze the subject system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

52. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices, (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

    a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system

software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

c. I am familiar with and understand the implications of the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that any of the materials to be searched and seized from the SUBJECT PREMISES are protected materials pursuant to the PPA. If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

Conclusion

53. Based on the above information, there is probable cause to believe that evidence of the previously mentioned

federal violations have been violated and that the following property, evidence, fruits and instrumentalities of these offenses will be located at the SUBJECT PREMISES:

a. images of child pornography and files containing images of child pornography in any form wherever it may be stored or found including, but not limited to:

   i. any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to visually depict child pornography or child erotica; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child

pornography, or information pertaining to an interest in child pornography, child erotica or information pertaining to an interest in child pornography;

ii. books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iii. originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iv. and motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

b. information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

ii. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iii. credit card information including but not limited to bills and payment records;

iv. records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence; and

v. records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

54. Based upon the foregoing, this Affiant respectfully requests that this Court issue a search warrant for the SUBJECT PREMISES, more particularly described in Attachment A which is attached hereto and made a part hereof, authorizing the seizure of the items described in Attachment B, which is also attached hereto and made a part hereof.

55. It is further respectfully requested that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the

requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the SUBJECT PREMISES). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation, and premature disclosure of the contents of this Affidavit and related documents may jeopardize the effectiveness of this ongoing investigation.

56. The above information is true and correct to the best of my knowledge.

/s/ _____

Sean Lichner
Special Agent
Department of Homeland Security
Immigration & Customs Enforcement

Subscribed and sworn
before me this 5th of April 2004.

/s/ _____
JAMES B. TODD
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

1) 3813 Mimosa Lane
Lexington, Kentucky 40517

The promises is described as a two-story sided building, green in color, with an attached two-car garage. The front of the building has three windows, a doorway and the attached two-car garage facing Mimosa Lane. The premises is located on a culdasac.

ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

1. images of child pornography and files containing images of child pornography in any form wherever it may be stored or found including, but not limited to:

   i. any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

ii. books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iii. originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

iv. motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

2. information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

ii. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors

engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

3. credit card information including but not limited to bills and payment records;

4. records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence; and

5. records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

APPENDIX E

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
LEXINGTON

Case No. 04-5054M

[Filed April 8, 2004]

IN THE MATTER OF THE	)
SEARCH OF:	)
Tax Crises Center	)
Wagers Tax Firm, Inc.	)
1608 Harrodsburg Road	)
Lexington, Kentucky 40504	)
	)

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

I, Sean Lichner, being duly sworn depose and say:

I am a(n) Special Agent with the Department of Homeland Security, U.S. Immigration and Customs Enforcement and have reason to believe that __ on the person of or X on the property or premises known as the Tax Crises Center, Wagers Tax Firm, Inc., 1608 Harrodsburg Road, Lexington, Kentucky 40504, which is further described as a two story brick dwelling with eight window facing Harrodsburg Road. A white colored sign for the business located close to the

sidewalk near Harrodsburg Road. The business is described in Attachment A which is attached hereto and made a part hereof.

in the EASTERN District of KENTUCKY there is now concealed a certain person or property, namely a computer, computer hardware, and those items more specifically described in attachment "B" which is attached hereto and made a part hereof.

which is evidence of a crime, contraband, fruits of crime, other items illegally possessed, or property designed for use, intended for use, or used in committing a crime, concerning a violation of Title 18 United States Code, Section(s) 2252(b)(1), 2252(a)(2) & 2252(a)(4)(B).

The facts to support a finding of Probable Cause are as follows:

SEE Attached Affidavit of Special Agent Sean Lichner which is attached hereto and made a part hereof.

Continued on the attached sheet and made a part hereof.
✓ Yes ___ No

/s/ Sean Lichner

Signature of Affiant

Sworn to before me, and subscribed in my presence

April 8, 2004
Date

at Lexington, Kentucky
City and State

James B. Todd, U.S. Magistrate Judge
Name and Title of Judicial Officer

/s/
Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEARCH WARRANTS

I, Sean Lichner, being duly sworn, depose and state:

1. I am a Special Agent with the Department of Homeland Security, United States Immigration and Customs Enforcement (ICE), assigned to the Resident Agent In Charge Northern Kentucky. I have been so employed since April 7, 2003. As part of my daily duties as an ICE agent, I am responsible for investigations involving the importation and distribution of child-pornography and criminal violations relating to the sexual exploitation of children. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 United States Code ["U.S.C."] § 2256).

2. This Affidavit is made in support of an Application for a Search Warrant for the business location known as Wagers Tax Firm, Inc. The residential dwelling listed in paragraph (A) was searched pursuant to a federal search warrant on April 7, 2004.

   (A) As set forth above, on April 7, 2004, a federal search warrant was executed at Lyman Wagers' dwelling located at 3813 Mimosa Lane, Lexington, Kentucky 40517 (the "SUBJECT PREMISES"). During the search of the SUBJECT PREMISES a computer processing unit was located in an upstairs bedroom. A cursory search of the computer revealed several sexually explicit jpeg images of children and at least two m[illegible] videoclips of children engaged in sexually explicit conduct. The search agents also seized a

laptop computer and other electronic storage data which will be processed within the next few days to determine if there are additional images which would be prosecutable pursuant to Title 18, United States Code, Section 2252.

(B) The affidavit being submitted is for the business known as Wagers Tax Firm, Inc., located at 1608 Harrodsburg Road, Lexington, Kentucky 40504 (the "SUBJECT BUSINESS"), and is, for the most part the same affidavit submitted in support of the search of the residence set forth in paragraph 2(A). After searching the above residence, counsel for Wagers met with your affiant and others in an attempt to reach an accommodation on a search of the SUBJECT BUSINESS. The parties agreed that counsel for Lyman Wagers, Jr. would accompany the search agents to the SUBJECT BUSINESS. Because the SUBJECT BUSINESS is a tax business, the search agents will attempt to limit the search of any computers located at the SUBJECT BUSINESS to image files which might be located on the computers, or other electronic storage data. The search agents will also limit the search to any printed images, videotapes, or other materials listed in detail in this affidavit and in Attachment "B" which is incorporated in this affidavit and is attached to the search warrant. The SUBJECT BUSINESS is more particularly described as a two-story red-brick building with eight windows and the front door facing Harrodsburg Road. There is a sign outside the business labeled "Wagers Tax Firm, Inc."

3. The purpose of this application is to seize evidence of violations of Title 18, United States Code, Sections,

2252(b)(1), 2252(a)(2) and 2252(a)(4)(B), for a conspiracy to receive, attempt to receive, the receipt and the possession of child pornography, respectively. Based on the facts set forth in this affidavit, I have reason to believe that evidence of the previously listed criminal violations will be found at the locations listed in paragraph 2.

4. Title 18, United States Code, Section 2256, defines the term child pornography as meaning "means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where

   (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

   (B) such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct;

   (C) such visual depiction has been created, adapted, modified to appear that an identifiable minor is engaging in sexually explicit conduct; or

   (D) such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

5. Title 18, U.S.C., Section 2256(2) defines sexually explicit conduct as meaning "actual or simulated

(A) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

(B) bestiality;

(C) masturbation;

(D) sadistic or masochistic abuse; or

(E) lascivious exhibition of the genitals or pubic area of any person;"

6. I am familiar with the information contained in this Affidavit based upon the investigation I have conducted, the investigation of other law enforcement officers and conversations with other law enforcement officers who have engaged in numerous investigations involving child pornography.

7. As a result of the investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, as set for the above will be located at the SUBJECT BUSINESS.

8. The investigation has revealed that an individual employing the e-mail account Spike20004u@aol.com, subsequently identified as Lyman E. WAGERS, Jr., purchased at least four (4) subscriptions to websites that were distributing child pornography, and that there is probable cause to believe that Spike20004u@aol.com subscribed to these websites using computers that are located at the SUBJECT PREMISES and at the SUBJECT BUSINESS.

9. The information set forth below is provided as a broad overview of the investigation conducted to date. It does not include a listing of all investigative techniques employed or even the full and complete results of any of the listed investigative efforts.

Overview of the Underlying New Jersey Investigation

10. The United States Attorney's Office for the District of New Jersey ("USAO DNJ"), the U.S. Department of Justice's Child Exploitation and Obscenity Section ("CEOS"), and the New Jersey offices of ICE, Internal Revenue Service, Criminal Investigations Division ("IRS CID"), the United States Postal Inspection Service ("USPIS"), and the Federal Bureau of Investigation ("FBI") conducted a joint investigation (the "New Jersey Investigation") of Regpay, a third-party billing and credit card aggregating company. The investigation revealed that Regpay conspired with other website operators to commercially distribute child pornography by providing the other websites with billing and credit card aggregating services, and taking a percentage of the other websites' illegal proceeds. The investigation also revealed that Regpay itself operated several websites that sold child pornography.

Regpay's Billing Service Operations for Child Pornography Websites

11. The New Jersey Investigation revealed that (1) Regpay operated regpay.com, a website that it used to conduct its billing services; (2) the regpay.com website was housed on a server at Verio, Inc.; (3) Regpay leased IP addresses at Rackspace Managed Hosting ("Rackspace"), and Regpay housed its customer databases including customer

transaction records on servers at Rackspace; (4) Regpay obtained the assistance of Connections USA, Inc. ("Connections"), a Florida Domestic Corporation located in Florida, to coordinate its billing and credit card processing services; and (5) Connections processed at least $3,000,000 for Regpay between November 1, 2002 and April 30, 2003 including credit card transactions that Connections processed for Regpay through Iserve.com ("Iserve")[1], an e-commerce company that purportedly provides a variety of payment processing services, including the performance of credit card and check processing, for computer websites that offer membership subscriptions to the public. During the course of the New Jersey Investigation of Regpay, federal agents, acting in an undercover capacity ("the UC Agents") became paid subscribers/members of websites that used Regpay as a billing company.[2] In many instances, when a UC agent subscribed to a website or purchased a membership to a website using a credit card, a billing page automatically appeared on the computer screen, which sought personal and financial information, and revealed that the transaction was being processed by or through Regpay. At the top of the billing page was a logo containing the letters "rp" and the word "regpay," as well as the name of the website to which the undercover agent was seeking to subscribe or purchase. After completing the form, which included providing a credit card number to be used for the purchase, each UC agent was instructed to "hit the

---

[1] Iserve.com is a fictitious business name owned by Connections.

[2] The investigation revealed that not all of those websites used Regpay exclusively; some of those websites used multiple billing companies.

JOIN NOW! button" on the screen. Shortly after clicking on the "JOIN NOW!" button, each UC agent received a message from Regpay stating that Regpay successfully charged the provided credit card. The message provided each agent with a transaction number, log-in information, and a password to log into the members-only site. The message stated that "Iserve will appear on your credit card statement as a beneficiary of this transaction." In some instances, shortly after receiving the above described message from Regpay, the agent/purchaser also received a message from "Iserve.com," thanking the customer for using Regpay, and indicating that Iserve would appear on the customer's billing statement. The message thereafter provided the date and time of the transaction, a transaction number, and the amount of the transaction. Records later obtained from the banks that issued the credit cards used in several of the undercover purchases listed "Iserve" for each of these transactions.

12. As part the New Jersey Investigation of Regpay, information housed on various servers that helped facilitate customer transactions for hundreds of websites was seized from several locations in the United States pursuant to several search warrants. After analyzing the customer data, the ICE forensic agents identified tens of thousands of purchases of child pornography between January 2003 and July 2003 associated with those websites, that is tens of thousands of confirmed subscriptions which granted purchasers access to those websites.

13. Further, undercover purchases made by ICE agents (described above in paragraph 11) prior to executing search warrants for Regpay's customer transactional information, were found to be recorded in the database

found on Regpay's Rackspace server. ICE forensic specialists determined that the Regpay database operated under a database management system called "MySQL," and that this database's contents and structure were thus legible. In other words, upon finding that the database operated using the MySQL system, and that the coding was intelligible, ICE forensic experts determined that they could decipher Regpay's customer transactional data and use it to identify the subscribers/members of the websites to whom Regpay had provided third-party billing services.

14. At various times between February and September 2003, federal agents verified that at least 21 websites that Regpay had been servicing were still active, accessible on the Internet, and contained child pornography. They did so by accessing these websites on the Internet and subscribing to those sites that advertised child pornography or showed actionable images in their "preview" or "nonmember" sections. Although the federal agents have no way of ascertaining the actual contents of each website on the various dates customers would have visited the websites, the federal agents were able to verify that on those dates the websites were visited by the federal agents, the websites contained child pornography as defined by federal law.

15. Based on the customer transaction records obtained through the execution of search warrants which revealed customer subscriptions to websites that federal agents had independently verified as containing child pornography, the ICE Cyber Crimes Center identified various individuals as subscribers to websites containing child pornography. In turn, the ICE Cyber Crimes Center sent leads to field offices across the country. The search

warrant of the SUBJECT PREMISES and SUBJECT BUSINESS evolved from one of those leads.

ICE Analysis of Regpay's Customer Transactional Data

16. By way of background, and as noted earlier, Regpay's customer transactional information was found to be recorded in the database found on Regpay's Rackspace server, which was searched pursuant to a warrant. ICE forensic specialists examined the source code[3] or 'scripts' used to populate the various fields in the Rackspace database, and determined how each of the fields pertaining to the websites' customers (hereinafter, "subscriber(s)/member(s)") were generated by Regpay's web page programming.

17. The ICE forensic specialists learned that when Regpay had served as the billing company for the members-only websites that contained child pornography, the subscribers/members of these websites would input certain information when a billing page would appear. That information was then recorded by Regpay in fields that it maintained in its database.

18. The fields that appeared in the Regpay customer information data, which ICE forensic specialists determined had been completed based upon information provided by the websites' subscribers/members were:

---

[3] Source code is computer software programming statements and instructions.

1. fname, referring to the website subscriber/ member's first name as entered on the Regpay form;

2. lname, referring to the website subscriber/ member's last name of the customer as entered on the Regpay form;

3. addr, referring to the website street address as entered on the Regpay form;

4. city, referring to the website subscriber/member's city as entered on the Regpay form;

5. state, referring to the website subscriber/member's state as entered on the Regpay form;

6. zip, referring to the website subscriber/member's zip code as entered on the Regpay form;

7. phone, referring to the website subscriber/ member's telephone number as entered on the Regpay form;

8. country; referring to the website subscriber/ member's country as entered on the Regpay form;

9. ccnumber, referring to the website subscriber/member's credit card number as entered on the Regpay form;

10. cvv2, referring to the website subscriber/ member's three digit number from the credit card, as entered on the Regpay form;

11. card_type, referring to the website subscriber/ member's credit card, as entered on the Regpay form;

12. expmonth, referring to the website subscriber/ member's credit card, as entered on the Regpay form;

13. expyear, referring to the website subscriber/ member's credit card expiration date, as entered on the Regpay form; and

14. email, referring to the website subscriber/ member's e-mail address as entered on the Regpay form.

19. Federal agents who had subscribed, in their undercover capacity, to one or more websites containing child pornography, and whose transactional information was found to be among the consumer transaction data seized during the searches of Rackspace's Regpay servers, verified that the information pertaining to the transactions they had conducted was contained as each of them had input it in the Regpay database.

20. ICE Cyber Crime Center determined that a field in the "members" table of the Regpay database called "siteid" was a unique identifier that correlated each subscription purchase to a website listed in the "sites" table of the database. ICE agents were able to determine which website each customer purchased by correlating the siteid entry in the "members" table to the relevant "sites" table entry.

21. In addition to determining which fields were completed by subscribers/members, forensic specialists at ICE's Cyber Crime Center also determined that the following fields on the Regpay customer transaction forms were generated automatically by Regpay's coding or script, and then stored in Regpay's MySQL database:

    (a) login, referring to the access user name;

    (b) passwd, referring to a randomly generated 8 character password; and

    (c) regtime; referring to the hour:minute:second the script ran (according to the host machine).

22. The fact that the fields referenced in paragraph 21 were computer-generated and were relayed to subscribers/members prior to their entry into the purchased websites is significant. Based on my own experience and conversations with other agents, although a website subscriber/member could easily provide a false name when subscribing to websites, the subscriber/member most certainly had to provide a legitimate credit card number and an e-mail account in order to subscribe to/become a member of the website. This is because the subscriber/member would have been required to provide a valid e-mail account in order to actually enter the website in which he or she was interested in. In fact, entry into the members-only websites that contained child pornography would most likely have been preceded by the subscriber/member's receipt of an e-mail that, along with confirmation that the credit card purchase had been successfully completed, included the subscriber/member's computer-generated password, as well as instructions needed to access the

website (see paragraph 11). Inaccurate credit card or e-mail information would most likely have precluded entry into the website. Given the likely accuracy of the e-mail address and credit card information provided by the subscriber/member, federal agents focused on that information to identify subscribers/members.

Probable Cause to Search the Subject Premises

23. Upon receipt of a lead from the ICE Cyber Crimes Center, the undersigned affiant, working with other agents in the Ft. Mitchell Field Office, the United States Postal Inspection Service and the Kentucky State Police commenced an investigation, which revealed that between June 30, 2002 and June 3, 2003, an individual whose e-mail address is Spike20004u@aol.com, with reported addresses of 1608 Harrodsburg Road, Lexington, Kentucky 40504, and 3813 Mimosa Lane, Lexington, Kentucky 40517 who used credit card numbers are 3712 7076 9432 006 and 4427 4203 4012 6520, subsequently identified as Lyman E. WAGERS, JR, paid to subscribe to four (4) websites later confirmed to contain child pornography. Based on the investigation and my training and experience, there is probable cause to believe that WAGERS is a recipient and collector of child pornography, and that evidence of his conspiracy to receive, attempt to receive, the receipt and the possession of child pornography will be found at his residence, the SUBJECT PREMISES, and at his business, THE SUBJECT BUSINESS.

24. More specifically, in the course of analyzing the Regpay customer transactional data that had been seized pursuant to the search warrants referenced above, it was discovered that one of the individuals who was a subscriber to the

following members-only websites: http://redlagoon.com, http://www.video2000.com/ and http://www.darkfeeling.com, used and e-mail account of Spike20004u@aol.com. The investigation further revealed that the individual using the e-mail account/user name[4] Spike20004u@aol.com, provided addresses of 1608 Harrodsburg Road, Lexington, Kentucky 40504 and 3813 Mimosa Lane, Lexington, Kentucky 40517 and the telephone number 859-271-3483. This individual used a series of credit cards to purchase access to members-only websites between June 30, 2002 and June 3, 2003, including, but not limited to, a card issued by American Express Travel Services ("American Express") and a card issued by Bank One NA ("Bank One").

25. The customer transaction records indicate that four of the members-only sites' purchased by Spike20004u@aol.com permitted electronic access to child pornography. Specifically, Spike20004u@aol.com purchased access to the following members-only sites on or about the following dates:

    1. http://redlagoon.com - June 30, 2002;

---

[4] An e-mail account/user name/screen name is the name a person uses to identify himself or herself when logging onto a computer system or online service. Both a username (user ID) and a password are required. Typically, with an Internet e-mail address, the user name is the address that precedes the @ sign. For example, harryW is the username in harryW@usdoj.gov. ISPs call the username a "screen name." For purposes of the instant affidavit, the undersigned Affiant has used the terms "user name" (or, in the case of AOL, "screen name"), and "e-mail account" interchangeably.

2. http://www.Video-2000 - March 22, 2003;

3. http://www.dark-feeling.com - April 15, 2003; and

4. http://www.Video-2000 - June 3, 2003.

26. From on or about February 26, 2003 though on or about August 02, 2003, federal agents made the following undercover purchases of memberships to websites containing child pornography:

(i) **www.redlagoon.com/lustgallery aka www.lust-gallery.com:** On March 26, 2003, a federal agent, while acting in an undercover capacity, purchased a one-month membership, in the approximate amount of $49.95 + additional fees, to a website entitled "Lust Gallery". A credit card number was provided to effect this transaction. The information appearing in the address box of my internet browser, while viewing the subscription page was http://64.239.16.69/sale.cgi?s=91111&ad=ad00094313. The name "regpay" appeared in relatively large letters on the webpages as the main billing company and on the approval page in smaller type was the name "ISERVE", which was listed as the "beneficiary of this transaction".

Additional information on the approval page included the transaction number: 178628, a login: me01793961, a password: 4YHdhagp, and a members UBL of http://69.0.255.118/members/. Using this information, the undercover agent accessed the website and downloaded images of children engaged in sexually explicit conduct.

Contained on the website were numerous pictures depicting minor females in various poses and states of undress. Specifically, three of the images contained on the website are described as follows:

1. 35&back=30: This image features a pubescent, nude female raising the left leg of a second prepubescent, nude female, exhibiting the genitals of the second prepubescent female.

2. 7&back=0: This image features a closeup of the genital and anal area of a pubescent nude female with her legs apart exhibiting her genitals.

3. 31&back=30: This image features a closeup of the genital area of a pubescent nude female squatting on the floor with her legs spread apart.

(ii) On August 1, 2003, a federal agent, while acting in an undercover capacity, purchased a 31 day membership to a website entitled "Video-2000" aka www.video-2000.com, site URL name http://www.video-2000.net/members/index/html using master card gift card number 553772001581390 for approximately $50.90. The membership was purchased with a credit card provided to a billing company identifying itself as Cardspay. Cardspay thereafter provided the agent with a login number, password, and the member URL site with the web address: http://www.video-2000.net/members/index/html. Using this information, the agent accessed the website and

downloaded videos of children engaged in sexually explicit conduct.

(iii)**http://www.darkfeeling.com:** On July 21, 2003, a federal agent, acting in an undercover capacity, purchased a one-month membership, for approximately $57.90, to a website with a URL of www.darkfeeling.com. The undercover agent used a MasterCard credit card. This credit card information was provided to a billing company identifying itself as "Regpay". Regpay thereafter provided the agent with a transaction number: 295276, a login: me01901415, a password: sTh8mbXM, and members URL of http://69.0.237.222/members. Using this information, the undercover agent accessed the website and downloaded images of children engaged in sexually explicit conduct. The home page of the website features images of several females of various ages in multiple poses, and an invitational to become a member of the website. Contained within the website were numerous pictures of young girls in various poses and states of undress. Specifically, three of the images contained in this website are described as follows:

1. DSCN8577.jpg in Set #79: This image features a nude prepubescent female sitting in a chair. Her right leg is bent at the knee and her leg is leaning slightly outward, her left leg is bent at the knee and is lying out to the side, parallel to the floor. Her legs are parted in approximately a ninety degree angle, her genital area is exposed as well as her undeveloped breasts. Her left hand is grasping her left shin. The photo was taken from a frontal viewpoint.

2. P1010370 Set #67: This image features a nude prepubescent female lying on a bed on her back with her legs spread apart, exposing her genital area. Her left-leg is bent at the knee and is leaning out to the side, her right leg is outstretched, lying flat against the bed.

3. DSCN2327.jpg Set #60: This image features a nude prepubescent female sitting on what appears to be a shag carpet on the floor. The nude prepubescent female is leaning back against an item of furniture with her legs spread apart, exposing her genital area. Both of her legs are bent up at the knees and are parted, leaning out away from her body. Her hands are grasping her ankles.

27. The undersigned Affiant reviewed several DVD disks sent to the Ft. Mitchell ICE field office, which contained digitally preserved copies of the above-listed websites purchased by undercover agents. The undersigned Affiant has also personally reviewed the content of the above websites purchased by Spike20004u@aol.com, that were digitally preserved and the content copied to the hard drive by ICE Agents at the Cyber Crimes Center in Fairfax, Virginia. An agent with expertise in the field of child pornography reviewed several images from each of those websites and concluded that they constitute child pornography.

28. America Online, Inc. ("AOL") is an ISP through which the user name Spike20004u@aol.com was issued. A Subpoena was sent to AOL following the receipt of the lead from the Cyber Crimes Center. Records returned from AOL as a result of the Subpoena indicate that the e-

mail address Spike20004u@aol.com is associated with Lyman WAGERS whose billing address is 1608 Harrodsburg Road, Lexington, Kentucky 40504, the SUBJECT BUSINESS.

29. AOL also confirmed that WAGER'S account was activated on November 24, 2000; that the account was active at the time that each of the purchases described above were made; and that WAGERS gave a night phone number of 859-271-3483 and a day phone number of 859-276-0594.

30. AOL also provided the following screen names/e-mail accounts that belong to WAGERS: cruelsadistm, k9trainer4yf, leewagers2001 and slavemasterlee.

31. The AOL billing records indicate that the method of payment for AOL services for WAGERS use of AOL is by a Visa credit card. The number listed on the AOL billing records is 4427 4203 4012 6520. This Visa card number is identical to WAGER'S Bank One card number that was listed in the Rackspace customer records.

32. On or about June 30, 2002, WAGERS purchased access to http://redlagoon.com. The customer transaction records from Rackspace indicate list the IP address of the computer that was accessing http://redlagoon.com as 172.150.168.17. A trace of the IP address using the website ARIN WHOIS reveals that the IP address is owned by AOL.

33. Insight Communications ("Insight") is an ISP that is utilized by WAGERS. Records returned from Insight following the issuance of a Subpoena reveal that WAGERS utilizes high speed internet access at the

SUBJECT PREMISES and also has video programming. The billing addresses listed on the WAGER'S Insight records are 3813 Mimosa Lane, Lexington, Kentucky, the SUBJECT PREMISES and 1608 Harrodsburg Road, Apt. A, Lexington, Kentucky, the SUBJECT BUSINESS. Additionally, Insight provides several telephone numbers, including 859-27 1-3483 as the number listed to 3813 Mimosa Lane, Lexington, Kentucky, the SUBJECT PREMISES and 859-276-0594 as the number listed to 1608 Harrodsburg Road, Apt. A, Lexington, Kentucky, the SUBJECT BUSINESS.

34. Insight also confirmed that WAGER'S account was activated on October 9, 2002 and that the account was active at the time that each of the purchases described above were made.

35. On March 22, 2003 a purchase was made for access to http://www.video2000.com. The IP address that a computer used to access the Internet to purchase a membership was listed on the customer transaction records as 12.222.198.103. On April 15, 2003, a purchase was made for access to http://www.darkfeeling.com. The IP address of the computer that accessed the Internet to purchase a membership to http://www.darkfeeling.com was listed on the customer transaction records as 12.222.198.103. On June 6, 2003, a purchase was made for access to http://www.video2000.com. The IP address of the computer that accessed the Internet to purchase a membership was listed on the customer transaction records as 12.222.198.103. The information Insight provided to Agents/Officers as a result of a Grand Jury Subpoena reveals that the IP address 12.222.198.103 was

assigned to Lyman E. WAGERS JR. during the time period from March 6, 2003 to June 3, 2003.

36. Following receipt of the lead from Newark, it was determined that the purchase made for access to http://redlagoon.com on June 30, 2002 was made with WAGER'S card number 3712 7076 9432 006. The purchase price, according to the Rackspace records, was $67.90. The card number was identified as being issued by American Express. A Subpoena was sent to American Express for financial and ownership records for card number 3712 7076 9432 006. The records returned from America Express list the card owner as Lyman E. WAGERS JR. with an address of 1608 Harrodsburg Rd., Lexington, Kentucky 40504-3706. The American Express account for WAGERS was activated on December 13, 1996 and is currently an active account. The financial records returned from American Express list two charges to "ISERVE FT. LAUDERDALE FL" on June 27, 2002. Both charges were in the amount $67.90. Furthermore, according to American Express, card number 3712 7076 9432 006 was not reported lost or stolen during the period of the purchases.

37. Pursuant to the receipt of the information from the Cyber Crimes Center, it was determined that the purchase made for access to (i) http://www.video2000.com on March 22, 2003; (ii) http://www.darkfeeling.com on April 15, 2003; and (iii) http://www.video2000.com on June 3, 2003 were made with card number 4427 4203 4012 6520. This card number was identified as being a checking card issued by Bank One. A Subpoena was sent to Bank One for financial and ownership records on card number 4427 4203 4012 6520. The records returned from Bank One list Wagers Tax Firm Inc. as the primary account holder

for card number 4427 4203 4012 6520 with a billing address of 1608 Harrodsburg Road, Lexington, Kentucky 40504. The account number is listed as 615074150 and the type of account is listed as a Bank One business checking account. WAGERS signed the business signature card as President of Wagers Tax Firm Inc. The card was activated on January 3, 2003 and is currently active. Furthermore, the Bank One Subpoena Compliance Department has indicated that there were no disputes reported during the time period that included the three purchases referenced above.

38. The Bank One financial records list a charge to "Iserve *8009290300" on March 21, 2003 in the amount of $67.90. This charge corresponds to the March 22, 2003 listing found in the Rackspace records for access to http://www.video2000.com. The Rackspace records list the amount paid as $67.90.

39. The financial records from Bank One list a charge for "Iserve *8009290300" in the amount of $82.90 on April 14, 2003. This is within a day of the listing in the Rackspace records for a purchase made by WAGERS for in the amount of $82.90 for access to http://www.darkfeeling.com. The amount listed in the Rackspace records for the WAGERS'S purchase of access to http://www.darkfeeling.com is also listed as $82.90.

40. The financial records from Bank One list a charge on June 2, 2003 for Iserve *8009290300. The financial records list the charge as $67.90. The records found with Rackspace list a purchase made by WAGERS on June 3, 2003 for access to http://www.video2000.com. The Rackspace records list the amount paid for access to http://www.video2000.com as $67.90.

41. A further review of the Bank One financial records show that in addition to the charges for Iserve referenced above, charges for ISERVE appear eight (8) additional times between February 6, 2003 and June 21, 2003. The fact that Iserve appears eight (8) additional times on WAGER'S Bank One financial records is relevant to the underlying investigation. Your affiant has learned through discussions with other agents and officers and that over a over majority of Iserve's business consisted of third party billing for web sites that allowed access to child pornography for a fee.

42. A study of the monthly billing records for Bank One shows that the card has over twenty-five (25) charges from third party billing services. Specifically, at least fifteen (15) charges relate to Rigva, Latvia and St. Petersburg, Russia. Based on your affiant's experience with the New Jersey investigation and discussions with other agents and officers, it is known that countries in the former Eastern block region, including Latvia and Russia, are source countries for child pornography that appears on the Internet.

43. Additional information obtained from public databases reveals that WAGERS lives at 3813 Mimosa Lane, Lexington, Kentucky 40517 and has a home phone number of 859-271-3483 and business phone number of 859-276-0594.

44. A Commonwealth of Kentucky, Department of Motor Vehicles check revealed that Lyman E. WAGERS, JR., Date of Birth, 12/23/1948, possesses a Commonwealth of Kentucky Drivers License. The check listed the WAGER'S address as 3813 Mimosa Lane, Lexington, Kentucky. Two vehicles are listed as registered to

businesses affiliated with WAGERS and/or WAGERS. The first, which is registered to Lyman Wagers PSC/Lyman Wagers, is a 2004 Lexus, green in Color, bearing Kentucky license plate number 2419JR, vehicle identification number JTJBT20X730004413. The second, which is registered to Wagers Tax Firm Inc./Lee Wager, is a 2000 Lexus, gold in color, bearing Kentucky license plate number 582FMA, vehicle identification number JT6HF10U5Y0113410.

45. A query of the Commonwealth of Kentucky online business database lists Lyman E. Wagers as the Incorporator, Registered Agent, and sole Officer of a Kentucky corporation known as Wagers Tax Firm, Inc. The address listed is 1608 Harrodsburg Road, Lexington, Kentucky 40504, the SUBJECT BUSINESS. The standing of the business is listed as being in good standing and the status is listed as active.

46. On October 31, 1997, Lyman Wagers entered a plea of guilty to a one count criminal Information charging him with a violation of Title 18, United States Code, Section 2252(a)(4)(B), for the possession of child pornography. Pursuant to Kentucky Supreme Court rules, Wagers was automatically suspended from the practice of law following his guilty plea. On December 18, 1997, the Kentucky Supreme Court entered an order automatically suspending Wagers from the practice of law effective November 1, 1997, pending further orders of the court. There is no indication that Wagers has resumed the practice of law. Notwithstanding Wagers' suspension from the practice of law, search team members will be briefed on the possibility that stored confidential files could be stored at either the business or residence. If such files are located, the files will immediately be

isolated and looked at by a separate search team to ensure that no confidential information is compromised. Any search of such records would be for the sole and limited purpose of determining if sexually explicit images were secreted with the any archived client files. Also, as a result of his conviction, Wagers is listed as a sex offender on the Commonwealth of Kentucky State Police Registry online database. WAGERS is listed as Lyman E. WAGERS, Jr., with a registration date of March 3, 1999. The registry lists WAGER'S address as 3813 Mimosa LN, Lexington, Kentucky 40517 as of December 1, 2003.

47. A Postal Inspector verified through the United States Postal Service database that WAGERS receives mail at 3813 Mimosa Lane, Lexington, Kentucky 40517 that is, the SUBJECT PREMISES and at 1608 Harrodsburg Road, Lexington, Kentucky 40504 the SUBJECT BUSINESS. Additionally, a postal carrier confirmed on January 17, 2004 that WAGERS has continued to accept mail at the SUBJECT PREMISES and that no other person is listed as a mail recipient at the SUBJECT PREMISES.

48. Surveillance of the SUBJECT PREMISES revealed that on March 1, 2004 and on March 12, 2004 a Lexus with license plate number 2419JR was parked behind the business during business hours.

49. Based upon the information provided by AOL, Insight, Bank One, American Express, The United States Postal Service, the Commonwealth of Kentucky State Police Sex Offender Registry, and the Kentucky Secretary of State, there is probable cause to believe that the individual using the user or screen name Spike20004u@aol.com is Lyman

E. WAGERS JR., who lives at the SUBJECT PREMISES and works at the SUBJECT BUSINESS.

50. Based on the foregoing there is probable cause to believe that records, documents and materials relating to WAGER'S receipt and possession of child pornography are located in WAGER'S residence, SUBJECT PREMISES and at the SUBJECT BUSINESS, Wagers Tax Firm, Inc.

Specifics Regarding the Seizure and Searching of Computer Systems

51. Based on my own experience and consultation with other agents who have been involved in the search of computers and retrieval of data from computer systems and related peripherals, and computer media, there are several reasons why a complete search and seizure of information from computers often requires seizure of all electronic storage devices, as well as all related peripherals, to permit a thorough search later by qualified computer experts in a laboratory or other controlled environment:

    1. Computer storage devices, such as hard disks, diskettes, tapes, laser disks, and Bernoulli drives, can store the equivalent of hundreds of thousands of pages of information. Additionally, when an individual seeks to conceal information that may constitute criminal evidence, that individual may store the information in random order with deceptive file names. As a result, it may be necessary for law enforcement authorities performing a search to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This review and sorting process can

take weeks or months, depending on the volume of data stored, and would be impossible to attempt during a search on site; and

2. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even those who are computer experts to specialize in some systems and applications. It is difficult to know before a search what type of hardware and software are present and therefore which experts will be required to analyze the subject system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

52. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices, (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

c. I am familiar with and understand the implications of the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that any of the materials to be searched and seized from the SUBJECT PREMISES are protected materials

pursuant to the PPA. If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

Conclusion

53. Based on the above information, there is probable cause to believe that evidence of the previously mentioned federal violations have been violated and that the following property, evidence, fruits and instrumentalities of these offenses will be located at the SUBJECT BUSINESS:

a. images of child pornography and files containing images of child pornography in any form wherever it may be stored or found including, but not limited to:

i. any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup

tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to visually depict child pornography or child erotica; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, child erotica or information pertaining to an interest in child pornography;

ii. books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iii. originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iv. and motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

b. information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

ii. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iii. credit card information including but not limited to bills and payment records;

iv. records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence; and

v. records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

54. Based upon the foregoing, this Affiant respectfully requests that this Court issue a search warrant for the SUBJECT BUSINESS, more particularly described in

Attachment A ~~which is attached~~ hereto and made a part hereof, authorizing the seizure of the items described in Attachment B, which is also attached hereto and made a part hereof.

55. It is further respectfully requested that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the SUBJECT PREMISES). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation, and premature disclosure of the contents of this Affidavit and related documents may jeopardize the effectiveness of this ongoing investigation.

56. The above information is true and correct to the best of my knowledge.

/s/ _____

Sean Lichner
Special Agent
Department of Homeland Security
Immigration & Customs Enforcement

Subscribed and sworn
before me this 8th of April 2004.

/s/ _____
JAMES B. TODD
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

1) 3813 Mimosa Lane
Lexington, Kentucky 40517

The subject premises is described as a two-story sided building, green in color, with an attached two-car garage. The front of the building has three windows, a doorway and the attached two-car garage facing Mimosa Lane. The premises is located on a culdasac. The subject premises were searched on April 7, 2004.

2) 1608 Harrodsburg Road
Lexington, Kentucky 40504

The premises is described as two story red brick dwelling with eight windows facing Harrodsburg Road. A white colored sign for the business located close to the sidewalk near Harrodsburg Road reads:

Tax Crises Center
WAGERS
TAX FIRM, INC.
276-0594

ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

1. images of child pornography and files containing images of child pornography in any form wherever it may be stored or found including, but not limited to:

    i. any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

ii. books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iii. originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

iv. motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

2. information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

ii. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors

engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

3. credit card information including but not limited to bills and payment records;

4. records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence; and

5. records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

APPENDIX F

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
LEXINGTON

Case No. 04-5053M

[Filed April 8, 2004]

IN THE MATTER OF THE	)
SEARCH OF:	)
Any and all accounts in the	)
name of Lyman Wagers, 1608	)
Harrodsburg Road, Lexington,	)
Kentucky, maintained at the	)
offices of America OnLine Inc.,	)
22000 AOL Way, Dulles,	)
Virginia 20166	)
	)

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

I, Sean Lichner, being duly sworn depose and say:

I am a(n) Special Agent with the Department of Homeland Security, U.S. Immigration and Customs Enforcement and have reason to believe that __ on the person of or X on the property or premises known as (name, description and/or location)

in the EASTERN District of KENTUCKY there is now concealed a certain person or property, namely See Attachment A which is attached hereto and made a part thereof.

which is evidence of a crime, contraband, fruits of crime, other items illegally possessed, or property designed for use, intended for use, or used in committing a crime, concerning a violation of Title 18 United States Code, Section(s) 2252(b)(1), 2252(a)(2) & 2252(a)(4)(B).

The facts to support a finding of Probable Cause are as follows:

SEE Attached Affidavit of Special Agent Sean Lichner which is attached hereto and made a part hereof.

Continued on the attached sheet and made a part hereof.
✓ Yes ___ No

/s/ Sean Lichner

Signature of Affiant

Sworn to before me, and subscribed in my presence

April 8, 2004 at Lexington, Kentucky
Date City and State

James B. Todd, U.S. Magistrate Judge
Name and Title of Judicial Officer

/s/
Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Sean Lichner, being duly sworn depose and state:

1. I am a(n) Special Agent with the Department of Homeland Security, United States Immigration and Customs Enforcement (ICE), assigned to the Resident Agent in Charge Northern Kentucky. I have been so employed since April 7, 2003.

2. As part of my daily duties as an ICE agent, I am responsible for investigations involving the importation and distribution of child pornography. I have received training in the area of child pornography and child exploitation.

3. The purpose of this application is to seize evidence of violations of Title 18 United States Code (U.S.C.), Section 2252, for the receipt, distribution and possession of child pornography. Based on the facts set forth in this affidavit, I have reason to believe that evidence of violations of Title 18 U.S.C. 2252 will be found at offices of AOL, located at 22000 AOL Way, Dulles, Virginia 20166 for the account of Lyman E. WAGERS JR., 1608 Harrodsburg Road, Lexington, Kentucky 40504 or 3813 Mimosa Lane, Lexington, Kentucky 40517.

Probable Cause that child pornography will be found at AOL

Federal Agents investigate "Regpay" a company operating various members only child pornography websites

In or about February 2003, a federal undercover operation coordinated out of the District of New Jersey revealed that a company called "Regpay," located in Minsk, Belarus owned and operated various members only Internet websites containing images of what appeared to the agent in New Jersey to be real children engaging in pornographic conduct with other children and with adults.

In or about July and August 2003, federal agents acting in an undercover capacity obtained memberships to, and visited, these members only websites. The undercover agents confirmed by visiting the websites and purchasing memberships therein that these paid access websites advertised child pornography and that they contained extensive collections of child pornography.

Federal Agents Seize Regpay's Customer Transaction Records

In or about June, 2003, ICE agents from Florida seized and processed Regpays customer database. This database was housed on a server located in Texas. T he database contained Regpay's records for each customer who purchased access to one of Regpay's child pornography websites. The information included the purchasers name, home address, e-mail address, credit card number, names of websites purchased, and the date(s) of each purchase. The information was then distributed to various agents in different jurisdictions, including this one.

In or about July and August 2003, federal agents from the ICE Cyber Crimes Center, located in Fairfax, Virginia, with backgrounds in investigations relating to the sexual exploitation of children, visited all the above websites that WAGERS had purchase membership access to.

The agents determined that these websites contained extensive collections of sexually explicit photographic and video images of what appear to be real children posing and/or engaging in sexually explicit activities with other children.

In July and August 2003,the ICE agents in Virginia also captured the contents of these websites when they visited the sites. In January 2004 federal agents, including your affiant, reviewed the contents of the child pornography websites that WAGERS purchased membership access to, and confirmed that many of the images and videos on these websites depicted sexually-explicit activities involving minor girls and boys.

Lyman E. WAGERS JR. Identified as One of Regpay's Customers

Following receipt of the transaction records, federal agents discovered that Lyman E. WAGERS JR. was one of Regpay's paying customers, and that he subscribed to these websites using the e-mail address Spike20004u@aol.com. The records contained in Regpay's customer database for WAGERS is as follows:

Custom. Name	Custom. Address	Website	Custom. E-Mail	Purchase Date
Lyman Wagers	1608 Harrods-burg Rd. Lexing-ton, KY 40504	http://redlagoon.com	spike20004u@aol.com	6/30/02

Lyman Wagers	3813 Mimosa Ln. Lexington, KY 40517	http://www.lust-gallery.com	spike200004u@aol.com	3/6/03
Lyman Wagers	1608 Harrodsburg Rd. Lexington, KY 40504	http://www.video-2000.com/regpay/	spike200004u@aol.com	3/22/03
Lyman Wagers	3813 Mimosa Ln. Lexington, KY 40517	http://trust.teenboysarchive.com	spike200004u@aol.com	4/11/03
Lyman Wagers	1608 Harrodsburg Rd. Lexington, KY 40504	http://www.darkfeeling.com/	spike200004u@aol.com	/034/1
Lyman Wagers	1608 Harrodsburg Rd. Lexington, KY 40504	http://video-2000.com/regpay/	spike200004u@aol.com	6/3/02

AOL Provides Federal Agents with spike2004@Aol.Com Subscriber Information

Following the receipt of the Regpay customer transaction records, a Federal Grand Jury Subpoena was sent to AOL for subscriber and log information on spike20004@aol.com. On or about February 2, 2004, federal agents received a response from AOL. The response indicated that spike20004@aol.com was a name utilized by Lyman WAGERS. AOL also provided the following screen names/e-mail accounts that belong to WAGERS: spike20004u, cruelsadistm, kgtrainer4yf, leewagers2001 and slavemasterlee.

Review of Financial Records

In January 2004 federal agents contacted Bank One NA ("Bank One") and determined that WAGERS is the account holder of Bank One card number 4427 4203 4012 6520. The Regpay customer transaction records indicated that this card was used to obtain access to http://www.video-2000.com on March 22, 2003 and on June 3, 2003 and http://www.darkfeeling.com/ on April 15, 2003. Financial and Subscriber Records returned from Bank One as the result of a Federal Grand Jury Subpoena confirm that charges appeared on WAGERS account in the name of ISERVE. ISERVE is a fictitious business name associated with Connections USA, a Florida corporation that was one of several companies helping Regpay process payments for access to websites containing child pornography.

The purchase prices listed in the Regpay customer transaction records for purchases made for access to http://www.video-2000.com and http://www.darkfeeling.com/ match the amounts charged for Iserve as listed in the Bank One financial records.

In January 2004 federal agents contacted American Express Travel Services ("American Express") and determined that WAGERS is the account holder of Bank One card number 3712 7076 9432 006. The Regpay customer transaction records indicated that this card was used to obtain access to http://redlagoon.com. Financial and Subscriber Records returned from American Express as the result of a Federal Grand Jury Subpoena confirm that charges appeared on WAGERS account in the name of ISERVE in the amount of $67.90 on June 27, 2003.

Wagers Tax Firm, Inc.

The records returned from Bank One list WAGER'S address as 1608 Harrodsburg Road, Lexington, Kentucky, 40504. A query of the Commonwealth of Kentucky, Secretary of State Online Business Database, shows a listing for Wagers Tax Firm, Inc. 1608 Harrodsburg Road, Lexington, Kentucky, 40504. WAGERS is listed as the Incorporator, the sole Officer and sole Director for Wagers Tax Firm, Inc.

Internet Provider Used to Access Child Pornography Websites

The customer transaction records indicate purchases made for access to http://www.lust-gallery.com/, http://www.video-2000.com/regpay/, http://trust.teenboysarchive.com, and http://www.darkfeeling.com/ were made with a Computer using Internet Protocol ("IP") address number 12.222.198.103.

A trace of the IP address 12.222.198.103 with the website Arin Whols reveals that IP address 12.222.198.103 is owned

by Insight Communications. Insight Communications is an Internet Service Provider ("ISP"). A Federal Grand Jury Subpoena sent to Insight reveals that WAGERS utilizes high speed Internet access at 3813 Mimosa Lane, Lexington, Kentucky and that the billing addresses listed for the account are 1608 Harrodsburg Road, Lexington, Kentucky and 3813 Mimosa Lane, Lexington, Kentucky.

Insight also confirmed that WAGER'S account was activated on October 9, 2002 and that the account was active at the time that each of the purchases described above were made.

WAGERS is Sole Occupant of Residence

A Postal Inspector verified through the United States Postal Service database that WAGERS receives mail at 3813 Mimosa Lane, Lexington, Kentucky 40517 and at 1608 Harrodsburg Road, Lexington, Kentucky 40504.

On April 7, 2004, a federal search warrant was executed at the residence of Lyman Wagers, Jr. A preliminary search of a computer located in a bedroom at Wagers' residence revealed several image files and movie files which depicted minors engaged in sexually explicit activity. The files were located in a subdirectory which indicated the files were received through Wagers' AOL internet service.

Based on the information provided by AOL and Insight, a limited review of evidence recovered in the search of Wagers' residence on April 7, 2004, and the experience and training of other federal law enforcement agents involved in this investigation, your affiant believes that WAGERS uses the spike20004u@aol.com e-mail account to order, arrange for the payment of, and arrange for the receipt of child

pornography, and that probable cause exists to believe that evidence of violations of Title 18, U.S.C. Section 2252 is located at 22000 AOL Way, Dulles, Virginia 20166.

REQUEST FOR SEALING

This investigation is continuing and disclosure of the contents of this Affidavit will jeopardize the progress of the investigation. Accordingly, I request that the Court issue an order, pursuant to which, Search Warrant and Affidavit, as well as related documents, be filed under seal until further order of this court.

/s/ Sean Lichner

Special Agent, ICE

Subscribed and sworn
before me this 8th day of April, 2004.

/s/ James B. Todd
United States Magistrate Judge

LIST OF ITEMS TO BE SEIZED FROM AOL

1. All business records, in any form kept, in the possession of America online, Inc., 22000 AOL Way, Dulles, Virginia 20166, in the Eastern District of Virginia, which pertain to the account belonging to Lyman E. Wagers, Jr., 1608 Harrodsburg Road, Lexington, Kentucky 40504 and 3813 Mimosa Lane, Lexington, Kentucky, 40517, to include, but not limited to, the subscriber's full name, all screen names associated with that subscriber and account, all account numbers associated with that subscriber, method of payment, phone numbers and addresses and detailed billing records (listing date, time, duration, and screen name used each time a particular account is activated), and all e-mail sent to, sent from, or received by the subscriber.

2. All records of subscriber account preferences to include, but not limited to, "'Favorite Places," "Member Profiles" and "book marked" websites specified by the subscriber of the account, together with any "address books" or "Buddy Lists" maintained or related to the account.

3. All history of Customer Term of Service staff complaints against screen names associated with the above captioned account.

4. All electronic mail, images, whether adult or child and all text messages and other content stored on Lyman Wagers, Jr.'s account.

5. A complete log file of all activity relating to WAGERS accounts with AOL (including dates, times, method of connection, port, dial-up, dedicated phone number, an/or location).

6. All account information for any other accounts that are associated with WAGERS.

APPENDIX G

UNITED STATES CODE
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I. CRIMES
CHAPTER 110. SEXUAL EXPLOITATION AND OTHER ABUSE OF CHILDREN

18 USCS § 2252

§ 2252. Certain activities relating to material involving the sexual exploitation of minors

(a) Any person who–

(1) knowingly transports or ships in interstate or foreign commerce by any means including by computer or mails, any visual depiction, if--

(A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(B) such visual depiction is of such conduct;

(2) knowingly receives, or distributes any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution in interstate or foreign

commerce by any means including by computer or through the mails, if--

(A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(B) such visual depiction is of such conduct;

(3) either-

(A) in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the Government of the United States, or in the Indian country as defined in section 1151 of this title [18 USCS § 1151], knowingly sells or possesses with intent to sell any visual depiction; or

(B) knowingly sells or possesses with intent to sell any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means, including by computer, if--

(i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(ii) such visual depiction is of such conduct; or

(4) either--

(A) in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the Government of the United States, or in the Indian country as defined in section 1151 of this title [18 USCS § 1151], knowingly possesses 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction; or

(B) knowingly possesses 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if--

(i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(ii) such visual depiction is of such conduct;

shall be punished as provided in subsection (b) of this section.

(b)(1) Whoever violates, or attempts or conspires to violate, paragraph (1), (2), or (3) of subsection (a) shall be fined under this title and imprisoned not less than 5 years and not more than 20 years, but if such person has a prior conviction under this chapter, section 1591 [18 USCS § 1591], chapter 71, chapter 109A, or chapter 117 [18 USCS §§ 2251 et seq., §§ 1460 et seq., 2241 et seq., or 2421 et seq.], or under

section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to aggravated sexual abuse, sexual abuse, or abusive sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, or sex trafficking of children, such person shall be fined under this title and imprisoned for not less than 15 years nor more than 40 years.

(2) Whoever violates, or attempts or conspires to violate, paragraph (4) of subsection (a) shall be fined under this title or imprisoned not more than 10 years, or both, but if such person has a prior conviction under this chapter, chapter 71, chapter 109A, or chapter 117 [18 USCS §§ 2251 et seq., §§ 1460 et seq., 2241 et seq., or 2421 et seq.], or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to aggravated sexual abuse, sexual abuse, or abusive sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, such person shall be fined under this title and imprisoned for not less than 10 years nor more than 20 years.

(c) Affirmative defense. It shall be an affirmative defense to a charge of violating paragraph (4) of subsection (a) that the defendant--

(1) possessed less than three matters containing any visual depiction proscribed by that paragraph; and

(2) promptly and in good faith, and without retaining or allowing any person, other than a law enforcement

agency, to access any visual depiction or copy thereof--

(A) took reasonable steps to destroy each such visual depiction; or

(B) reported the matter to a law enforcement agency and afforded that agency access to each such visual depiction.